﴿ وَأَعِدُّوا لَهُم مَّا اسْتَطَعْتُم مِّن قُوَّةٍ وَمِن رِّبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ ﴾

١



العدد الأول - شهر ذو القعدة
سنة ١٤٢٧ هجرية

مجلة دورية تصدر عن مركز الفجر للإعلام

فن اخفاء الملفات

تحديد المواقع باستخدام الأقمار الاصطناعية

كيف تحمي بياناتك حتى لو تم اختراق جهازك

سلسلة الفيديو

سؤال وجواب

تعريف ببرنامج PGP وهل هو آمن بما فيه الكفاية للمجاهدين؟



المجلة تنشر حصريا في الحسبة والإخلاص والبراق والفردوس



لماذا مجلة المجاهد التقني ؟

ان مجلة المجاهد التقني تعنى بكل مايفيد المجاهد في الجانب الإعلامي من جهة و ورواد المنتديات الجهادية من جهة أخرى. فالمجلة تهتم بمتابعة الجديد والمفيد في أمن المعلومات وطرق حماية الحواسيب والمونتاج والهندسة الصوتية وأخبار الجهاد الإعلامي ورصد لأقاويل قادة الصليبيين حول أثر الجهاد الإعلامي عليهم ونحو ذلك .

و الأهداف التي نسعى الى تحقيقها باصدار المجلة هي :

1– نزع عقدة الخوف والهلع والموجودة في نفوس البعض والتي تحجزهم عن المشاركة بشكل فاعل في خدمة الجهاد لكون أحدهم يظن أن المخابرات يعدون عليه أنفاسه وحركاته فيعرّف بواقع الحال وبمبالغته فيعرف متى يقدم ومتى يحجم .

2– نشر الحس الأمني بشكل علمي لدى أعضاء المنتديات الجهادية من باب أخذ الحذر الذي أمرنا به بطريقة منطقية مرتبة وواقعية وبدون مبالغة أو تهوين

3– نشر الوعي التقني بكل مايفيد في مجال الإعلام الجهادي في مجال المونتاج المرئي والهندسة الصوتية و غيرها من أساسيات الاعلام

4– نشر مقالات علمية عن بعض التقنيات الحديثة التي من شأنها تطوير عمل الاخوة المجاهدين في الميدان

فريق العمل

رئيس التحرير : أبو المثنى النجدي

الكتاب المشاركون في العدد :أبو مصعب الجزائري , مجاهد اعلامي , أبو اسامة الشامي , أبو طلحة المصري , أبو الحارث الدليمي

تدقيق و مراجعة : أبومحمد المراكشي

الإخراج الفني : أبو الزبير المدني

تقرؤون في هذا العدد

الكلمة الافتتاحية

بسم الله الرحمن الرحيم

الحمد لله رب العالمين والصلاة والسلام على إمام المجاهدين نبينا محمد وعلى آله وصحبه أجميعن أما بعد.....

الحمد لله القائل في كتابه الكريم: (وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَمِنْ رِبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ)
والقائل:(وتعاونوا على البر والتقوى ولاتعاونوا على الإثم والعدوان)

والصلاة والسلام على نبيه الأمين القائل:"إن المؤمن يجاهد بسيفه ولسانه"
والقائل:"جاهدوا المشركين بأموالكم وأنفسكم وألسنتكم"

إن مجلة المجاهد التقني هي محاولة جادة ومسلك جديد لصد العدوان عن المسلمين ونصرة المجاهدين لإعلاء كلمة الله فوق كل أرض وتحت لك سماء

إن مجلة المجاهد التقني مجلة جهادية تهتم بالجانب التقني تحديداً .وهي محاولة أولية الهدف منها فتح الطريق للطاقات الكامنة لدى أنصار الجهاد لتنفجر و ينتج عنها ما ينفع أمتنا الإسلامية.

إن مجلتنا تستهدف نوعين من القراء و هما:رواد المنتديات الجهادية و المجاهدون الإعلاميون في الثغور.فالمجلة تسعى الى حماية رواد المنتديات تقنياً و زيادة مهارات استخدام الحاسوب لديهم حتى يصبحوا أعضاء فاعلين في الإعلام الجهادي.و في نفس الوقت شرح أحدث التقنيات التي من شأنها خدمة المجاهدين الإعلاميين.

قد تلحظون في المجلة الإهتمام بشكل أكبر بالأمن على شبكة الإنترنت وذلك لأنها مسألة حياة أو موت للمجاهدين فشبكة الإنرنت كانت فرصة ذهبية لاتقدر بثمن للمجاهدين بحيث استطاعوا كسر الطوق الذي فرضه الإعلام الصليبي وذنبه العميل في بلاد الإسلام واستطاع المجاهدون أن يطوعوها لخدمة الجهاد ونصرة الدين.

تعتمد المجلة على نوعين من الكتاب وهم:الكتاب الدائمون والذين نشرت مقالات بعضهم في هذا العدد و الكتاب الذين نتوقع مراسلتهم لنا بما يظنوا أن فيه نصرة للمجاهدين ومساعدة لرواد المنتديات .

ونحن في هيئة التحرير حين نبدأ العدد (الأول) في شهر ذي القعدة من عام 1427 هـ ، نتطلع إلى ذلك اليوم الذي نرى فيه هذه الوليدة وقد كبرت وشبّت وأصبحت مرجعاً أساسياً لجميع الإخوة المشاركين في المنتديات

كما إننا في هيئة التحرير نتطلع إلى المزيد من التطوير والتحديث لأبواب المجلة من حيث الشكل والمضمون،إلا أننا مهما بلغنا من الحرص على ذلك فلا بد من حدوث بعض القصور فهذه طبيعة العمل البشري، فلذلك سنكون نحن أعضاء هيئة التحرير في غاية السعادة عندما نتلقى آراءكم واقتراحاتكم فيما يختص بتطوير المجلة شكلاً ومضمونا ، فنحن نرى فيكم عوناً لنا تمدوننا بالمشاركات، وعيناً لنا ترصدون أخطاءنا وتنيرون الطريق لنا.

كما أننا في هيئة التحرير ننتهز هذه الفرصة لدعوة جميع من يقرأ هذه المجلة من المسلمين إلى المشاركة معنا والمساهمة بمقالاتهم العلمية، حتى نرقى بمستوى هذه المجلة إلى المعالي بإذن الله.

إننا في القرن الحادي والعشرين فليس لنا مكاتب ثابتة أو بريد تقليدي بل مجلتنا هذه تنشر حصرياً على شبكة الإنترنت ولنا بريد إلكتروني خاص نستقبل عليه الرسائل وسيتم إيصالها لآلاف المشتركين وتنشر حصرياً في أهم المنتديات الجهادية في العالم وهي التي يتم النشر فيها حالياً من قبل مركز الفجر للإعلام الذي نعمل تحت لوائه

بقي أن نذكر أن مجلة المجاهد التقني تصدر عن مركز الفجرللاعلام (وهو المركز المكلف رسمياً بنشر بيانات عدد من الجماعات الجهادية في أنحاء العالم وعلى رأسها إخواننا في تنظيم القاعدة بأفغانستان وإخواننا في دولة العراق الإسلامية ببلاد الرافدين وغيرها من الجماعات الجهادية المباركة) ومجلتنا الطيبة هذه وجه من أوجه الاستجابة لدعوة الشيخ أبي حمزة المهاجرأمير تنظيم القاعدة في بلاد الرافدين حول دعوته للخبراء والمتعلمين لنصرة الدولة الإسلامية الوليدة في بلاد الرافدين.

وإننا ماضون في حربنا هذه مع أعداء الله فوق كل أرض وتحت كل سماء حتى تحرر جميع أراضي المسلمين من رجس اليهود المعتدين والصليبيين الحاقدين ويكون الدين كله لله ونرى راية الإسلام خفاقة في الأرض.

والله أكبر والعزة لله ولرسوله وللمؤمنين....

يسعدنا تلقي إستفساراتكم ورسائلكم و مقالاتكم على بريد المجلة
http://teqanymag.arabform.com

أخوكم / رئيس التحرير
أبوالمثنى النجدي



فن إخفاء الملفات:

بقلم: أبو طلحة المصري



الحمد لله رب العالمين، والصلاة و السـلام على خير الأنبياء والمرسلين سيدنا محمـد، وعلى آله و أصحابه الطيبين الطـاهرين، ومن تبعهم بإحسان إلى يوم الدين.

أما بعد..

في هذه المقالة سنقوم باستعراض أسـاليب إخفاء الملفـات عـن أعـين البـاحثين، وسنستعرض ميزات كل أسلوب و عيوبه، مع شرح المهم من طرق إخفاء الملفات...

فباسم الله نبدأ و به نستعين :

إنه قد أصبح بحكم المعلوم ما لإخفاء الملفات من أهمية عظيمة في عصرنا الحاضر، وخاصة بعد أن تحوّلت جميع أنظمة المعلومات من الكتابة اليدوية إلى استخدام الحاسوب، ولكن في الحالة الجهادية فإنه تبرز حاجة ماسة للحفاظ على سرية المعلومات خوفاً من حصول الأعداء عليها مما يؤدي إلى مضارّ عظيمة في المسيرة الجهادية.

العوامل المؤثرة على طرق إخفاء الملفات :

إن عملية إخفاء الملفات تعتمد بشكل أساسي على مجموعة من العوامل، وبناءً على هذه العوامل يتم اختيار الطريقة الأمثل لإخفاء الملفات، وهنا سيتم تقديم شرح بسيط لكل عامل من هذه العوامل.



1) **توفر شبكة الإنترنت**: وهي تعني توفر خدمة الإنترنت عند من يريد إخفاء الملفات، وهذه الخدمة قد تكون سريعة أو بطيئة.

2) **حجم الملفات المراد إخفائها**: وهو المساحة الكلية للملفات، وتَنَاسُب حجمها مع سرعة الانترنت، فلو كانت سرعة الانترنت للرفع Mb1 في الثانية .. فعندها تعتبر المساحة MB 800 مساحة عادية حيث من الممكن رفعها في حوالي ساعتين.

3) **درجة الشك**: والمقصود هنا أنه في حالات الفحص العابرة والتي لا يوجد فيها شك مسبق كحالات الانتقال من بلد إلى آخر لشخص عادي مثلاً فإنه في هذه الحالة درجة شك المباحث في المطار بوجود معلومات على الجهاز تكون قليلة مما يجعلهم يستخدموا طرقاً بسيطة في فحص الجهاز. والعكس في حالة كشف جهاز في مركز للمجاهدين، فان أساليب التدقيق المستخدمة تكون متطورة نوعا ما وذلك لأن درجة الشك تكون عالية.

طرق الإخفاء بناءً على العوامل السابقة:

1) **إخفاء الملفات خارج جهاز الحاسوب:**

وهذه تعد أفضل وأسلم طريقة على الإطلاق، وهي أن تخزن معلوماتك في مكان يصعب أو يستحيل على خصمك الوصول له على الحقيقة.

وهذه الطريقة بسيطة وسهلة للغاية، وتتلخص بأن تقوم برفع ملفاتك إلى أحد سيرفرات الإنترنت في سينغافورة مثلاً، ويتم ذلك عبر استئجار موقع استضافة مجاني أو غير مجاني ورفع ملفاتك عليه، مع ملاحظة أهمية تشفير الملفات وضغطها بكلمة سر قبل الرفع.

والميزة الأساسية لهذه الطريقة هي توسيع مجال البحث للعدو ليشمل كل السيرفرات في العالم وليس الحاسوب الشخصي فقط، وهذه بالتأكيد أنجع الطرق وأفضلها.



و يفضل هنا أن يكون الموقع مستأجراً – وليس مجانيّا – إذا كانت المعلومات مهمة لضمان عدم ضياعها.

ويلاحظ هنا وجوب توفر العامل الأول المتمثل باتصال الإنترنت، والعامل الثاني المتمثل بمناسبة مساحة ما يراد إخفاؤه مع سرعة الإنترنت.

و هذه باختصار الخطوات السريعة اللازمة للقيام بهذه العملية:

1) نقوم بضغط الملف \ الملفات، باستخدام أي برنامج ضغط مثل **winrar** أو **winzip** .
2) نقوم بتشفير الملف باستخدام أحد برامج التشفير؛ مثل برنامج **ChaosMash 2.0** المشروحة طريقة عملـــه في الجزء الخامس من سلسلة أمن المجاهد التقني .
3) نقوم بإرسال مفتاح فك التشفير عبر الإيميل إلى أحد الإيميلات التي تُصنع لهذا الغرض. و هنا يجب ملاحظة أنه يمنـــع أن يكون المفتاح لفك التشفير والملف المشفر في نفس المكان – أي في نفس الجهاز. و يجب مراعـــاة تكـــبير حجـــم المفتاح قدر الإمكان.
4) يتم رفع الملف المشفر إلى أحد مواقع الرفع أو إلى موقع استضافة مجاني أو مستأجر. (طريقة الرفع متوفرة و بكثرة في المنتديات).

2) <u>إخفاء الملفات داخل جهاز الحاسوب :</u>

و هنا سيتم شرح طريقتين تستخدمان عند عدم توفر شبكة الانترنت، أو توفرها دون وجود تكافؤ بين حجم الملفات وسرعة الانترنت.

الطريقتان اللتان سيتم شرحهما هنا لكل منهما خصائص وميزات مهمة، وتعتمد على وضع المادة المراد إخفاؤها.

ولنبدأ بشرح الطريقة الأولى ...



أ) Alternative Data stream (ADS) :

هذه الطريقة تعد بامتياز أسهل الطرق لإخفاء الملفات في الجهاز، ورغم سهولتها الشديدة إلا أن استخداماتها عديدة وغير معروفة عند معظم الناس.

هذه الطريقة تقوم على بعض التقنيات الموجودة في نظام ملفات **NTFS** التابع لويندوز اكس بي أو ويندوز **2000**، حيث أنه عندما تم صناعة نظام الملفات هذا كان من المفروض أن يتوافق مع نظام الملفات التابع لنظام (أبل) فظهرت نتيجةً لذلك هذه التقنية. وبغض النظر عن الأسباب التي أدت إلى صناعة هذه التقنية فلنبدأ بشرح طرق استخدامها:

1) إخفاء الملفات بهذه الطريقة :

لنفترض أن لدينا ملفاً اسمه **test2.mpg** ونريد إخفاء هذا الملف في جهاز الحاسوب بحيث يستحيل كشفه بالنسبة لأي شخص ..
تقوم هذه الطريقة على إخفاء هذا الملف داخل ملف آخر (نظرياً) دون أي تغيير في حجم الملف الآخر أو الحجم الكلي للملفات التي في الجهاز، وهذه تعد أهم ميزات هذه الطريقة.

ولتطبيق الطريقة ما عليك سوى أن تقوم بكتابة الأمر التالي:

C:\type test2.mpg > test1.txt : test2.mpg

هذا الأمر ينسخ الملف **test2.mpg** الذي حجمه **660** كيلوبايت إلى الملف **test1.txt** الذي حجمه أقل من **1** كيلوبايت دون التأثير على حجم الملف **test1.txt** ، وهذا يظهر جلياً في المثال التالي :




```
G:\test>dir
 Volume in drive G has no label.
 Volume Serial Number is 9042-9155

 Directory of G:\test

07/15/2006  11:32 PM    <DIR>          .
07/15/2006  11:32 PM    <DIR>          ..
07/15/2006  08:09 PM                25 test1.txt
06/10/2006  01:36 AM           677,888 test2.mpg
               2 File(s)        677,913 bytes
               2 Dir(s)  5,604,761,600 bytes free

G:\test>type test2.mpg > test1.txt:test2.mpg

G:\test>dir
 Volume in drive G has no label.
 Volume Serial Number is 9042-9155

 Directory of G:\test

07/15/2006  11:32 PM    <DIR>          .
07/15/2006  11:32 PM    <DIR>          ..
07/15/2006  11:49 PM                25 test1.txt
06/10/2006  01:36 AM           677,888 test2.mpg
               2 File(s)        677,913 bytes
               2 Dir(s)  5,604,761,600 bytes free

G:\test>_
```

لاحظ المساحة الفارغة في الهارديسك

هذا هو الأمر

لاحظ أن المساحة لم تتغير

ويلاحظ هنا أن التغير الوحيد الذي طرأ على ملف test1.txt هو تاريخ الإنشاء.

الآن بإمكاننا إلغاء الملف الأصلي و الإبقاء على الملف المخفي، وهذا الملف المخفي يمكن استخدام جميع أوامر (الدوس) عليه مباشرة.

وفي المثال التالي نقوم بإلغاء الملف الأصلي ثم نقوم بتشغيل الفيلم عبر أحد برامج عرض الأفلام :

```
G:\test>del test2.mpg

G:\test>dir
 Volume in drive G has no label.
 Volume Serial Number is 9042-9155

 Directory of G:\test

07/16/2006  12:08 AM    <DIR>          .
07/16/2006  12:08 AM    <DIR>          ..
07/15/2006  11:49 PM                25 test1.txt
               1 File(s)             25 bytes
               2 Dir(s)  5,605,441,536 bytes free

G:\test>"C:\Program Files\K-Lite Codec Pack\Media Player Classic\mplayerc.exe" t
est1.txt:test2.mpg

G:\test>_
```

نلغى الملف الأصلى

هذا هو أمر تشغيل الفيديو من الدوس



فيظهر لنا الفيديو و قد عمل بنجاح :



و بنفس الطريقة؛ لو كان الملف المخفي ملف نصي نستخدم برنامج المفكّرة (**notepad**) أو الوورد في فتحه كما في المثال السابق، ونحتاج فقط أن نعرف مكان وجود المفكّرة أو الوورد في الجهاز.

حتى هذه النقطة نكون قد انتهينا من عملية إخفاء الملفات واستخدامها بهذه الطريقة، ولكن بقي علينا شرح كيفية إلغاء الملفات المخفية، وشرح ميزات ومضار هذه الطريقة.

2) حذف الملفات المخفية:

وهنا لدينا حالتان:

- إما أن يكون الملف الذي أخفينا فيه الملف وهمياً وليس ذا أهمية، عندها بمجرد إلغاء الملف الوهمي نكون قد ألغينا الملف المخفي. كما في مثالنا السابق فلو قمنا بإلغاء الملف **test1.txt** فإننا نكون أيضا قد ألغينا الملف المخفي الذي هو **test2.mpg**

- و الحالة الثانية والتي نكون فيها قد أخفينا الملف داخل ملف آخر مفيد كأحد ملفات النظام مثلاً عندها طريقة الإلغاء تكون كما يلي بناء على المثال السابق:



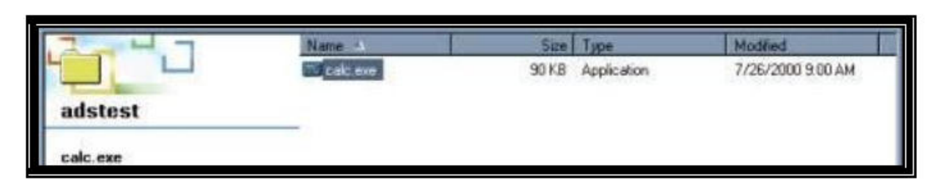
```
G:\test>ren test1.txt temp.txt
G:\test>type temp.txt > test1.txt
G:\test>del temp.txt
```

وهنا الملف temp.txt هو ملف مؤقت لتنفيذ هذه العملية.

3) استخدامات أخرى لهذه الطريقة (للمعلومة فقط وليست في صلب الموضوع):

في الحقيقة إن أكثر أنواع الاستخدامات لهذه الطريقة هو في عمليات اختراق الأجهزة؛ فمن المهم للمخترق إخفاء ملفاته وبرامجه في جهاز الضحية. و هذه الطريقة تعد من أسهل الطرق لهذا الغرض.

وهنا سأعرض مثالاً لإخفاء برنامج المفكرة (**notepad**) في برنامج الآلة الحاسوبة، وسأوضح أنه حتى عند محاولة إظهار البرامج التي تعمل في الجهاز فلن تظهر الآلة الحاسوبة.



الملف الذي سوف يخفى فيه برنامج المفكرة (notepad)

```
 Directory of C:\adstest

02/14/2004  04:47p      <DIR>          .
02/14/2004  04:47p      <DIR>          ..
07/26/2000  09:00a              91,408 calc.exe
               1 File(s)         91,408 bytes
               2 Dir(s)     684,425,216 bytes free

C:\adstest>type c:\winnt\system32\notepad.exe>calc.exe:notepad.exe

C:\adstest>dir
 Volume in drive C has no label.
 Volume Serial Number is 8C3F-115B

 Directory of C:\adstest

02/14/2004  04:47p      <DIR>          .
02/14/2004  04:47p      <DIR>          ..
02/14/2004  04:51p              91,408 calc.exe
               1 File(s)         91,408 bytes
               2 Dir(s)     684,371,968 bytes free

C:\adstest>
```

عملية الاخفاء كما شرحت مسبقا

نقوم بعملية الإخفاء كما شرح مسبقاً



نقوم بتشغيل البرنامج المخفي باستخدام الأمر start

كما هو ظاهر البرنامج الذي يظهر أنه يعمل هو الحاسبة رغم أن البرنامج الذي يعمل في الحقيقة هو notepad

4) العيوب والمساوئ :

ربما لا يوجد لهذه الطريقة من عيوب سوى أنها أصبحت شهيرة؛ مما أدى إلى ظهور برامج متخصصة للكشف عن الملفات المخفية بهذه الطريقة، وربما أشهرها برنامج يدعى LADS.



ولكن تذكّر أن هذه الطريقة تعد فعالة للغاية في حال عدم وجود شك كبير بك وفي حالات الفحص العابرة. فلــو كنت مثلاً تريد السفر من دولة إلى أخرى فإن هذه الطريقة تعد خياراً مقبولاً، حيث من الصعب على الجمــارك أن يقوموا بفحص الجهاز باستخدام برامج الكشف عن الــ **ADS**.

ومما يجب ذكره أيضاً أن هذه الطريقة لا تعمل إلا على الأقراص بنظام ملفات **NTFS** ، أي النظام لويندوز اكس بي وويندوز **2000**.

5) المميزات :

السهولة التامة وعدم تطلب الخبرة للتعامل بها.

و ميزة أخرى لها أنها غير مرتبطة ببرامج معينة مما يعني أنه حتى لو قمنا بإزالة القرص الصلب من الجهاز وفحــصنا القرص الصلب على جهاز آخر فإن هذا لن يؤدي إلى كشف الملفات المخفية دون استخدام برامج البحث عن الــ **ADS**.

ب) استخدام برامج الرووتكت **rootkit**

ملحوظة: هذه الطريقة تعد متطورة نوعًا ما، وهناك تداخل شديد بينها وبين الاختــراق وصــناعة الفيروســات والتروجانات . فإن كنت مبتدئاً في استخدام الحاسوب فأنصحك بشدة بعدم محاولة تجربة هذه الطريقة.

هذه الطريقة تعد متطورة إلى حد كبير، وهي تعتمد على ما يسمى الــ (**rootkit**)، وعمل الرووت كت يقوم على ما يلي:

- يقوم الرووت كت بضرب نظام التشغيل في جهاز المستخدم بحيث أنه يمنع نظام التشغيل (ويندوز مــثلاً) مــن عرض بعض الملفات أو تشغيل بعض البرامج ونحو ذلك.
- وأهم ما يميز الرووت كت أنه لا يظهر بتاتاً فالجهاز سيبقى يعمل بشكل طبيعي للغاية، وربما يستمر الــشخص بالعمل على الجهاز سنين دون أن يلاحظ أن فيه رووت كت.



- إذن، فالرووت كت هو وسيلة مستخدمة من قبل الهكر أو القراصنة لإخفاء معلومات وبــرامج علــى جهــاز الضحية دون أن يلاحظ الضحية أي شيء على جهازه .

و هنا في هذه الفقرة سنقوم نحن بأنفسنا بإنزال الرووت كت على أجهزتنا الشخصية، مع التحكم التام بها بحيث نجعلــها تؤدي الوظيفة التي نريدها منها، ألا وهي إخفاء الملفات دون الإضرار بالجهاز.

1) برامج الرووت كت :

هناك برامج عديدة للرووت كت ومعظمها يستخدم من قبل الهكر لاختراق الأجهزة. وهناك أنواع مــن الــرووت كت تأتي على شكل برامج خدمية، مثل برامج إخفاء الملفات، حيث أن معظم هذه البرامج في الحقيقة أنــواع مــن الرووت كت .

إن الرووت كت التي سوف يتم استخدامها هنا في هذا الشرح تسمى "**Hacker Defender Rootkit**" ، وهي رووت كت مفتوحة المصدر، وتعد الرووت كت الأساسية والأوسع انتشاراً والتي يتفرع منها معظم إصدارات الرووت كت.

طبعا هذه الرووت كت التي سيتم الشرح عليها مشهورة، وهذا يؤدي إلى أن معظم برامج مكافحــة الفيروســات سوف تمنعك من تشغيلها على الجهاز، ولكن إذا تم تشغيلها وبرنامج مكافحة الفيروسات لا يعمل فإنه حينئذ يعجــز تماماً عن كشفها.

ومما يستوجب ذكره أنه هناك نسخاً غير مجانية من هذه الرووت كت لا يمكن لأي برنامج اكتشافها، وتعد الآن من أخطر برامج الرووت كت .

2) طريقة عمل الرووت كت :

إن الرووت كت التي سنشرحها هنا تحتوي على ملف تنفيذي قابل للتشغيل، بالإضافة إلى ملف نصي.
وطريقة عملها أننا نقوم بوضع الخيارات في الملف النصي ككلمة السر والمجلدات التي نريد حجبها ونحــو ذلــك، ثم نقوم بتشغيل الملف فيختفي الملف والملف النصي وكل المجلدات التي طلبنا إخفاءها، ولا يمكن أن تظهر إلا بعد إيقاف الرووت كت بالأمر الذي سيتم شرحه لاحقاً .



و لنبدأ بشرح الخيارات في الملف النصي الآن.

3) الخيارات المتاحة

الخيارات المتاحة كثيرة و لكن سيتم هنا شرح الخيارات المهمة لنا:

أ) جدول المخفيات **(Hidden Table)**:

و هنا في هذا القسم يتم وضع لائحة بأسماء الملفات التي نريد إخفاءها، وكذلك المجلدات. والإمكانيات المتاحة في هذا القسم هي كالآتي:

1. إخفاء جميع الملفات والمجلدات التي تبدأ بكلمة معينة. كمثال على ذلك لو أردنا إخفاء جميع الملفات التي تحتوي على كلمة جهاد نكتب الآتي: **jehad*** ، وهذه تخفي كل الملفات التي تحتوي على كلمة جهاد في أولها أو آخرها أو في وسطها.
2. إخفاء ملف محدد في مكان محدد مثل **c:\fajr\abomosab.jpg** ، وهنا إما أن نقوم بإخفاء المجلد كله، أو إخفاء اسم الملف إذا كان الاسم فريداً.
3. إخفاء مجلد ما بما فيه مثل **C:\fajr** .

طبعا يجب ملاحظة هنا أنه بالإضافة للملفات التي نريد إخفاءها فإننا يجب أيضاً أن نقوم بإخفاء ملف الرووت كت, وهو في هذا المثال اسمه **hxdef100.exe**.

و مثال على هذا القسم من الملف يكون كالآتي:

```
[Hidden Table]
*hxdef
rcmd.exe
jehad*
abomosab.jpg
fajr
```



ملاحظة : فى هذه القائمة يمنع وضع العنوان الكامل للمجلد أو الملف المراد اخفاؤه وإنما يُكتفى باسمه فقط

مثلا: إذا كنا نريد إخفاء c:\fajr فإننا نضع فى القائمة fajr فقط دون ال\:c

ب) جدول المشغلات (**processes**) المخفية (**Hidden Processes**):

و هذا القسم مرتبط أكثر بعملية الهاك وعلاقته بنا محدودة في حاجتنا إلى إخفاء الرووت كت نفسها.

و هذا الجزء من الملف من المفترض أن يبقى كما هو في هذا المثال:

```
[Hidden Processes]
*hxdef
rcmd.exe
```

ج) جدول المشغلات (**processes**) الجذرية (**Root Processes**):

و هذا القسم مرتبط أيضاً بعمليات الاختراق إلا أن له فائدة بالنسبة لنا, ففي هذا القسم يتم وضع البرامج التي من المسموح لها عرض الملفات المخفية, فلو وضعنا هنا مثلاً **CMD.exe** فإن هذا يعني قدرتنا علــى عرض الملفات المخفية من الدوس حتى لو كانت الرووتكت تعمل.

و لعدم حاجتنا في هذا المثال لعرض الملفات بأي برنامج في حالة تشغيل الرووت كت فسيكون شكل هــذا القسم من الملف كالآتي:

```
[Root Processes]
*hxdef
rcmd.exe
```

د) جدول الخدمات المخفية (**Hidden Services**):

وهذه أيضاً غير مهمة لنا وهي تعني أنه في حالة عرض الخدمات **Services** التي تعمل على الجهــاز قــم بإخفاء الخدمات التالية .....



و هذا القسم يبقى كما هو:

[Hidden Services]
*HackerDefender

ه) جدول مدخلات الريجستري المخفية و جدول قيم الريجستري المخفية :

لعدم حاجتنا لهذين القسمين فلن يتم التغيير فيهما, و يبقيان كالآتي:

[Hidden RegKeys]
HackerDefender100
LEGACY_HACKERDEFENDER100
HackerDefenderDrv100
LEGACY_HACKERDEFENDERDRV100

[Hidden RegValues]

و) جدول البرامج التي في بدء التشغيل للرووت كت :

هنا يوضع البرامج المراد تشغيلها مع الرووت كت مثل (الباك دوور) والفيروسات وغيرها، وهي غير ذات أهمية لهذا الموضوع و عليه تترك خالية:

[Startup Run]

ز) المساحة الخالية :

هذا القسم مهم جداً لعملية إخفاء الملفات، فأحياناً يكون حجم الملفات المخفاة كبيراً جداً إلى درجة تدعو إلى الريبة، فبالرغم من إخفاء الملفات فإن أي شخص يمكن له ملاحظة الملفات المخفية عن طريق المساحة الخالية في القرص الصلب .

وهنا تأتي وظيفة هذا القسم !! ، حيث أننا نقوم بحساب تقريبي لحجم الملفات المخفية في كل قسم من القرص الصلب (الهارد دسك)، ونقوم بوضع الحجم في هذا القسم .



كمثال عليه, لنفترض أن حجم المجلد c:\fajr حوالي 100 ميجا. إذن نحن نحتاج لأن نضيف إلى المساحة الخالية في القرص c: 100 ميجا . فنضيف السطر التالي :

[Free Space]
C:100000000

ونضيف أسطراً أخرى لـــ D: مثلاً و نحو ذلك.

ح) المنافذ المخفية :

هذه تترك خالية لأنها قد تساعد على اختراق جهازك

[Hidden Ports]

ط) الإعدادات العامة :

و هذه الإعدادات شرحها يطول، ولكن الشيء الوحيد المهم تغييره هو أولها وهو كلمة المرور، و هذه الكلمة هي بحد أقصى 16 حرفاً انجليزياً، ويفضل وضعها صعبة للغاية.

و هذه هي الإعدادات مع كلمة المرور fajr :

```
[Settings]
Password=fajr
exe.$كBackdoorShell=hxdef
_.-=[FileMappingName=_.-=[Hacker Defender]=-._
ServiceName=HackerDefender100
ServiceDisplayName=HXD Service 100
ServiceDescription=powerful NT rootkit
DriverName=HackerDefenderDrv100
DriverFileName=hxdefdrv.sys
```

إلى هنا تنتهي الإعدادات و يصبح الرووت كت قابلا للتشغيل و إظهار التجارب.

و قد تم إضافة ملف الإعدادات المُستَخدَم في هذه التجربة مع الإضافات



4) التشغيل و التجارب

نعود ونكرر أن هذه العملية ليست للمبتدئين، وأن التشغيل في بعض الحالات قد يؤدي إلى مشاكل لا تُحمد عقباها.

بعد إعداد ملف الخيارات كما هو موضّح في القسم السابق نكون جاهزين لمرحلة التشغيل.

a) تشغيل الملف

يتم باستخدام الأمر التالي :

hxdef100.exe [inifile]

و الــ **[inifile]** هو اسم ملف الإعدادات، وهنا في المثال المرفق اسمه **hxdef100.ini**

```
C:\>cd fajr

C:\fajr>cd hxdef100r

C:\fajr\hxdef100r>hxdef100.exe hxdef100.ini

C:\fajr\hxdef100r>_
```

b) نتائج ما بعد التشغيل

في هذه الصورة تظهر الملفات قبل الإخفاء :

```
 Volume in drive C has no label.
 Volume Serial Number is

 Directory of C:\

06/13/2006  11:31 PM                 0
02/06/2006  01:12 PM                 0
02/06/2006  01:12 PM                 0
02/06/2006  02:27 PM               512
03/10/2006  08:20 PM    <DIR>          Downloads
03/12/2006  03:34 AM    <DIR>
05/12/2006  10:04 PM    <DIR>
02/06/2006  09:07 PM    <DIR>          Temp
02/06/2006  09:07 PM    <DIR>
05/14/2006  01:16 AM    <DIR>          Program Files
05/14/2006  01:16 AM    <DIR>          WINDOWS
05/24/2006  10:03 PM    <DIR>
05/30/2006  09:17 PM    <DIR>
07/29/2006  08:50 PM    <DIR>
08/04/2006  09:12 PM    <DIR>          download
08/05/2006  04:17 PM    <DIR>          fajr
               4 File(s)            512 bytes
              12 Dir(s)   2,389,422,080 bytes free

C:\>
```



و نلاحظ هنا ظهور مجلد الفجر **fajr** و أن المساحة الخالية هي **2389422080**

وهذه الصورة تظهر الملفات بعد الإخفاء :

```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is

 Directory of C:\

06/13/2006  11:31 PM                 0
02/06/2006  01:12 PM                 0
02/06/2006  01:12 PM                 0
02/06/2006  02:27 PM               512
03/10/2006  08:20 PM    <DIR>          Downloads
03/12/2006  03:34 AM    <DIR>
05/12/2006  10:04 PM    <DIR>
02/06/2006  09:07 PM    <DIR>
02/06/2006  09:07 PM    <DIR>
05/14/2006  01:16 AM    <DIR>          Program Fi
05/14/2006  01:16 AM    <DIR>          WINDOWS
05/24/2006  10:03 PM    <DIR>
05/30/2006  09:17 PM    <DIR>
07/29/2006  08:50 PM    <DIR>
08/04/2006  09:12 PM    <DIR>          download
               4 File(s)            512 bytes
              11 Dir(s)   2,488,283,136 bytes fre
```

و هنا يظهر أن المجلد **fajr** قد اختفى و كذلك المساحة الخالية أصبحت **2488283136** وهي أكبر من المساحة الخالية الفعلية بحوالي **100** ميجا تقريباً.

c) <u>إيقاف التشغيل</u>

لإيقاف التشغيل يتم استخدام الأمر التالي :

Net stop HackerDefender100

ويلاحظ هنا أن الاسم **HackerDefender100** كنا قد أضفناه إلى قائمة الإعدادات فـإذا غيرنـاه هناك يجب تغييره هنا.

و بعد ذلك نذهب إلى مكان الرووتكت و نكتب الأمر:

Hxdef100.exe :-uninstall

كما هو واضح في الصورة أدناه :




```
C:\fajr\hxdef100r>cd \

C:\>net stop HackerDefender100
The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.

C:\>cd fajr

C:\fajr>cd hxdef100r

C:\fajr\hxdef100r>hxdef100.exe :-uninstall
```

ملاحظات مهمة قبل البدء بعملية الرووت كت /

1) كما ذكرنا سابقاً من ملاحظة عدم تسمية العنوان الكامل للملف والاكتفاء باسم الملف فقط.
2) يجب إيقاف الإنترنت في جميع الفترة التي يكون فيها الرووت كت مفعلاً لأنه يحتوي على ما يسمى backdoor ويمكن من خلاله الوصول لجميع ملفاتك إذا عرف الباسوورد لذلك يفضل إيقاف الإنترنت ما لم تكن له حاجة.
3) لفك ضغط الملف الذي يحوي على الرووتكت يجب إيقاف مضاد الفيروسات في جهازك فهو سيعرفه على أنه من أخطر أنواع الفيروسات.
4) نعود و نكرر أنه إذا لم تكن تعرف كيفية التعامل بإتقان مع الحاسوب فمن الأفضل لك عدم التجربة بالنسبة للرووت كت.

ج) مقارنة بين الطريقتين

- كل طريقة من الطريقتين السابقتين تتميز بميزات عن الأخرى قد تجعل المرء يستخدم كل واحدة منهما على حسب الموقف .



– فطريقة إخفاء الملفات عن طريق الــ **ADS** تتميز بميزة مهمة جداً، وهي أنها غير مرتبطة بنظام التشغيل وارتباطها يتعلق بنوع نظام الملفات. هذا يعني أنه لو تم إخفاء أي ملف بهذه الطريقة على قرص صلب في حاسوب (أ) ثم نقلنا القرص الصلب إلى حاسوب (ب) فان الملف سيبقى مخفياً. و هذه الميزة لا تتوفر في الرووتكت .

– أما الرووت كت فإنها تتميز بميزة استحالة كشفها ما دامت على نفس الجهاز، والطريقة الوحيدة لكشفها هي تغيير نظام التشغيل بنقل القرص الصلب إلى جهاز آخر. وهذه الميزة مهمة جداً في حال التنقلات و السفر. فلو كنت تريد إخفاء ملفات أثناء تنقلك بين الدول فهذه الطريقة هي الأفضل لعدم استطاعة الفحص السريع على إزالة القرص الصلب و فحصه على جهاز آخر.

و فيما يلي جدول مقارنة بين الأسلوبين ..

الخاصية	Alternative Disk system (ADS)	الرووتكت
مستوى التعقيد	سهلة	معقدة
سرعة التنفيذ (سرعة إخفاء الملفات)	بطيئة	سريعة
مستوى الخطورة على الجهاز	لا يوجد خطورة	كبير جداً
مدة الإخفاء الفضلى	طويلة جداً (يمكن أن تبقى الملفات مخفية مع استخدامها باستمرار)	قصيرة لصعوبة استخدام الملفات أثناء الإخفاء
سهولة الكشف من على نفس الجهاز	متوسطة باستخدام برامج خاصة	معقدة للغاية
سهولة الكشف من على جهاز آخر	متوسطة بنفس الطريقة السابقة	سهلة

و بهذا ينتهي شرحنا لفن إخفاء الملفات راجين من المولى أن يكون نافعا لكم ..



نظام تحديد الموقع بالأقمار الاصطناعية:

بقلم: أبو الحارث الدليمي

تعريف بنظام تحديد الموقع بالأقمار الاصطناعية :



إن أحد أفضل الأنظمة التي قدمتها هندسة الاتصالات لخدمة البشرية هو نظام تحديد الموقع بالأقمار الاصطناعية، وهو عبارة عن منظومة مكونة من **24** قمراً منتشرة في الفضاء حول مدار أرضي ارتفاعه حوالي **20** ألف كيلومتر، بالإضافة إلى **3** أقمار احتياطية. والشرح المقدم فيما يلي مبسط كي يتسنى للجميع معرفة آلية عمل نظام تحديد الموقع بالأقمار الاصطناعية.

وللعلم فإن نظام الاتصالات هذا تابع لوزارة الدفاع الأمريكية، ولكنه مفتوح للاستخدام العام العالمي، فالطيران المدني ونظام الملاحة البحرية يقوم أساساً على هذا النظام، بالإضافة إلى عدد كبير من الاستخدامات نذكرها فيما بعد.

وجهاز تحديد الموقع هو جهاز استقبال فقط بينما في حالة أجهزة الاتصالات بالأقمار الاصطناعية فيمكن للجهاز إرسال مكان وجوده لشركة الاتصالات (مثل الثريا).

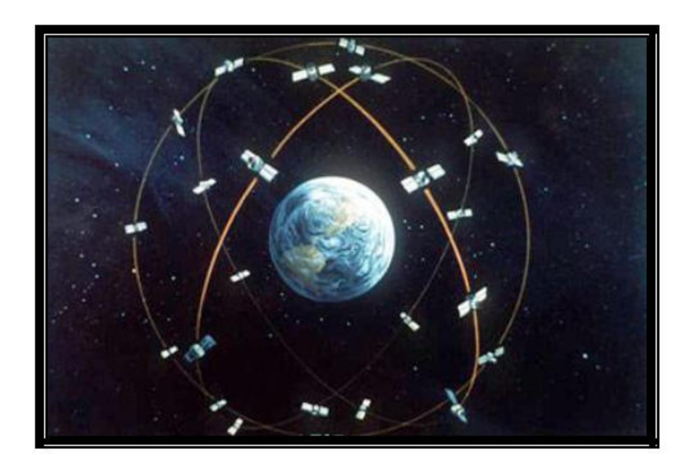
وأجهزة الاتصالات بالأقمار الاصطناعية هي أجهزة هجينة تدمج داخلها جهازين؛ الأول للاتصالات، والثاني لتحديد الموقع، و من هذا يتبين خطورة استخدام أجهزة هاتف الاتصالات عبر الأقمار الاصطناعية إلا في حدود ضيقة مع مراعاة تدابير السلامة. وللعلم فإن تحديد المواقع العسكرية و قصفها بدقة عالية يعتمد على تحديد موقعها بنظام جي بي إس.





صورة 1 : بعض تطبيقات تحديد الموقع بالأقمار الاصطناعية

هذه الأقمار تدور حول الأرض مرتين يومياً، وهي موزعة بحيث يمكنك في أي مكان وفي أي وقت استقبال إشارات من أربعة أقمار على الأقل. وجميع الأقمار تعمل بالطاقة الشمسية.



صورة 2 : توزيع شبكة أقمار تحديد الموقع حول الارض

وظيفة جهاز استقبال (جي بي إس) المحمول باليد (handheld GPS) – الذي هو عبارة عن جهاز حاسوب خاص مصغر– هي استقبال إشارات رقمية (Packets: data stream) من أربعة أقمار على الأقل، بعدها يقوم بحساب

المسافة التي تفصله عن كل قمر واستخدام هذه المعلومات لحساب موقعه بالنسبة للأرض. هذه العملية الحسابية تعتمد علـــى مبدأ رياضياتي يسمى (علم المثلثات).

كل إشارة يرسلها كل قمر تحتوي على موقع القمر بالنسبة للأرض بالإضافة للزمن عند القمر (يعتمد الزمن على ساعة ذرية موجودة في القمر الاصطناعي)، والزمن محدد بدقةِ نانو ثانية (نانو ثانية هي جزء من ألف مليون جزء من الثانية).

عند وصول هذه الرسالة (الإشارة الرقمية) لجهاز الاستقبال فإنه يمكنه حساب موقعه بالنسبة للقمر. وتتكرر هذه العملية مع أربعة أقمار على الأقل. وفي النهاية فإن الجهاز المستقبل يستطيع تحديد موقعه على الأرض بدقة عالية.

الإشارة المرسلة تقطع مسافة **30** ألف كلم في عُشر ثانية (**1/10**) و هي سرعة الضوء.

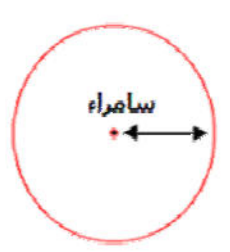


صورة 3 : جهاز استقبال بالأقمار الاصطناعية (**GPS receiver**) مجهز بنظام معلومات جغرافي (**GIS system**)

سنشرح فيما يلي مبدأ عمل جهاز استقبال جي بي إس في كيفية حساب الموقع. وللعلم فنظام جي بي إس يعمل في بيئة ثلاثيـــة الأبعاد وطريقة الحساب معقدة، بينما – تسهيلاً للشرح – سنشرح نفس الطريقة في بيئة ثنائية الأبعاد.

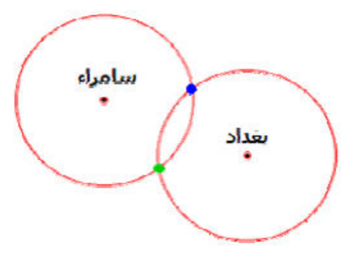
1. كيفية حساب الموقع من معلومات الأقمار:

نفترض أن شخصاً ما أخبرك أنك تبعد عن مدينة سامراء مسافة 60 كلم. هذه المعلومة لوحدها تعطيك مكاناً تقريبياً، لكنك لا تعرف هل أنت شرقاً أو غرباً، شمالاً أو جنوباً من المدينة، وهناك عددٌ لا متناهٍ من الاحتمالات. ومعنى ذلك أنك موجود في دائرة نصف قطرها 60 كلم حول مدينة سامراء ولا تعرف المزيد.



صورة 4 : تحديد الموقع باستخدام قمر واحد.

نفترض الآن أن شخصاً ثانياً قادم من مدينة بغداد أخبرك أنك تبعد عن بغداد مسافة 45 كلم.
الآن لو استخدمت المعلومتين؛ فرسمت دائرة حول سامراء (على الخارطة) نصف قطرها 60 كلم، و دائرة أخرى حول بغداد بنصف قطر 45 كلم؛ فإن تقاطع الدائرتين يعطيك احتمالين فقط لمكان و جودك (أنظر الصورة: نقطة زرقاء و نقطة خضراء).

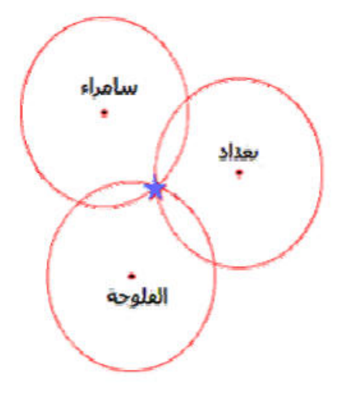


صورة 5 : تحديد الموقع باستخدام قمرين.



نفترض أن شخصاً ثالثاً قادم من الفلوجة أخبرك أنك تبعد عن الفلوجة مسافة **30** كلم. الآن لو رسمت دائرة ثالثة (على الخارطة) حول مدينة الفلوجة فإن تقاطع الدوائر الثلاث يحدد موقعك بالضبط (موقع النجمة الزرقاء).

نحتاج إذا لثلاثة أقمار لتحديد الموقع في بيئة ثنائية الأبعاد (**2-D** على الأرض)، ونحتاج إلى أربعة أقمار في بيئة ثلاثية الأبعاد (**3-D**) كون الأقمار موجودة في الفضاء وليست على الأرض. وكلما زاد عدد الأقمار التي يستطيع الجهاز استقبال الإشارات منها؛ كلما زادت دقة تحديد الموقع، والتي في التطبيقات العسكرية تقل عن المتر الواحد في دقة تحديد الموقع.!!



صورة 6 : تحديد الموقع باستخدام ثلاثة أقمار (النجمة الزرقاء).

المدن هنا هي أقمار اصطناعية، والأشخاص هم الإشارات التي ترسلها هذه الأقمار، حيث إنها ترسل – و بصورة متواصلة– موقع القمر (ورقمه) والزمن عند القمر بدقة تصل إلى جزء من ألف مليون جزء من الثانية (نانو ثانية). ومن المعلومات التي يرسلها كل قمر واعتماداً على سرعة الإشارة التي تبلغ **300** ألف كلم في الثانية فإن جهاز الاستقبال يقوم بمعالجة هذه المعلومات ليتوصل في الأخير إلى تحديد موقعه بدقة تصل إلى بضعة أمتار (تزيد أو تنقص حسب كون جهاز الاستقبال مدني أو عسكري) .

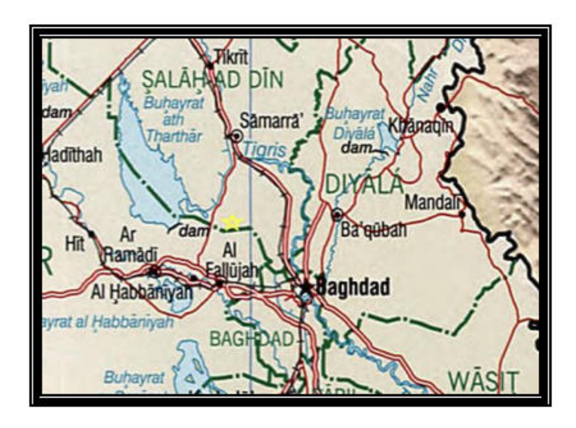
لغاية الآن شرحنا كيفية تحديد الموقع بالنسبة للأرض، وهذا الموقع يعتمد على خطوط الطول والعرض، فمثلاً الجهاز يعطيك موقعك: **36** درجة، **48** دقيقة و **14** ثانية بالنسبة لخطوط العرض، أما بالنسبة لخطوط الطول **42** درجة، **19** دقيقة و**20**

ثانية. (الدقائق والثواني هنا هي أجزاء من الدرجة وليست وحدة زمنية. تنقسم الدرجة إلى **60** دقيقة وتنقسم الدقيقة إلى **60** ثانية). طبعاً ليس كل شخص يستطيع فهم هذه القياسات ولكنها مستخدمة في علم الخرائط والأقمار الاصطناعية وعند العسكريين.

2. خرائط رقمية لنظام المعلومات الجغرافي (جي آي أس) :

يتم تحويل الخرائط الملتقطة بالأقمار الاصطناعية، وهي أقمار خاصة بالرصد الجيوغرافي والتصوير الجوي العسكري (موجودة في مدار يرتفع ألف كيلومتر فوق سطح البحر)، وهذه الخرائط الرقمية ذات أحجام كبيرة جداً، و إذا أردنا الحصول على خارطة للكرة الأرضية بدقة نقطية (**resolution**) تعادل نقطة لكل متر مربع (**$1m^2$ /pixel**) فإن حجم الصورة للكرة الأرضية يصبح **450** ألف جيغابايت (**450.000 GByte**)، والحجم هنا للصورة بشكل غير مضغوط، وهي كمية تخزينية خرافية.

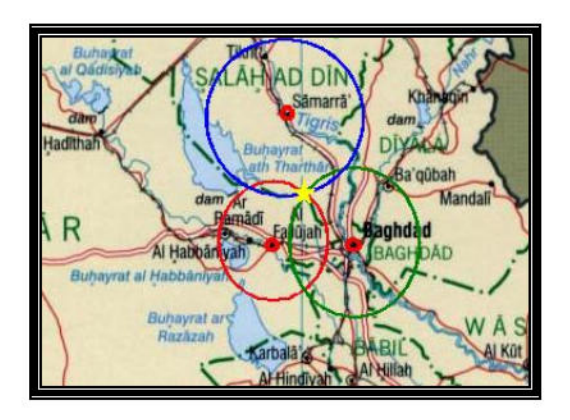
ولهذا فإن كل بلد له خارطته الرقمية منفصلة، ولا يمكن توفير خارطة لكل العالم. فمثلاً يمكنك شراء خارطة لفرنسا وأخرى للإمارات العربية، ولا تتوفر خرائط لكل أنحاء العالم، فمثلاً العراق و حده يحتاج لخارطة بحجم **500** جيغابايت، ولتصغير هذه الأحجام فإنه يتم أخذ خرائط للأماكن السكانية والطرقات المهمة، و يتم إهمال المساحات الشاسعة من الصحراء والمناطق الغير مأهولة.





3. دمج قياسات جي بي إس مع الخرائط الرقمية:

لتسهيل فهم القياسات والاستفادة منها بصورة فعالة لعامة الناس؛ يتم إدخال خرائط جغرافية رقمية للجهاز بحيث يقوم الجهاز بإسقاط معلومات الموقع (جي بي آس) على الخارطة الرقمية ليظهر لك موقعك على الخارطة مباشرة. ونظام الخرائط الرقمية هنا اسمه نظام المعلومات الجغرافي. وفيما يلي المثال السابق مسقطاً على خارطة العراق.



صورة 7 : دمج تحديد الموقع على خارطة جغرافية رقمية (جي بي إس – جي آي إس)

يبدو واضحاً أن تقاطع الدوائر هو النجمة الصفراء على الصورة. لكن هذه الدوائر هي تخيلية ولا تظهر على الجهاز.

هذه الأجهزة يستخدمها الطيران المدني ليحدد خطوط الطيران في الجو، و تستخدمها السفن للإبحار، و يستخدمها مهندسو الأراضي وعلم المساحة، وتستخدمها بعض السيارات الفارهة لمعرفة موقعها على خارطة الطرقات، ويستخدمها العسكريون لتحديد موقع آلياتهم على الأرض، وتستخدمها الصواريخ لضرب أهدافها بدقة.

الترددات الحاملة (**carrier frequencies**) التي يستخدمها نظام جي بي إس هي نوعان **1227** ميغاهرتز و**1575** ميغاهرتز. وطريقة التضمين (**Modulation**) تسمى : **Digital Sequence Spread Spectrum** ، وتختصر بـ **DSSS**، وهي تسمح للجهاز باستقبال إشارات ضعيفة جداً والاستفادة منها.



لكن كون جهاز الاستقبال يعمل بإشارات ضعيفة (مرسلة من أقمار تبعد مسافة تزيد عن **20** ألف كلــم) فإنــه بالإمكــان التشويش على هذه الأجهزة ومنعها من تحديد موقعها وخاصة في الاستخدامات العسكرية. فالآليات العسكرية من دون هذا النظام تتوه ولا تستطيع تحديد موقعها، وبالتالي سيتأخر وصول النجدة في حالة تعرضها لهجوم.

4ـ أجهزة ، معدات و أسعار:

بينما سعر جهاز جي بي إس المدني المجهز بخارطة جي آي إس (محلية خاصة بالولايات المتحدة) يــصل أو يزيــد عــن **1000** دولار؛ فإنه تتوفر قطع خاصة بالحاسوب المحمول بحيث يمكن الاستفادة من إمكانية الحاسوب بإضافة جهاز اســتقبال خــاص (صورة **8**) و تحويل الحاسوب المحمول إلى جهاز جي بي إس عالي الكفاءة، وسعر هذه القطعة أقل من **150** دولار. وميزة هذه القطعة الأخيرة أنه يمكن إخفاؤها بسهولة أثناء نقلها.

وفي حين أن نظام جي بي إس عالمي ولا يحتاج لأي تعديل إذا انتقلنا من بلد لآخر؛ فإن نظام المعلومات الجغرافي (جي آي إس) يحتاج للحصول على الخرائط الرقمية للبلد المرغوب. وهذه الخرائط التابعة لنظام المعلومات الجغرافي يتم تحميلــها في الجهــاز المحمول (**handheld GPS receiver**) أو في الحاسوب المحمول (صورة **10**). ويمكن الاستغناء عن الخرائط الرقمية إذا كان الشخص الذي يستخدم الجهاز مدرباً لذلك مثل العسكريين، ويكفي الاستعانة بخرائط خارجية (صــورة **9**) ونقــل الموقع الذي يعطيه جهاز جي بي إس على خارطة ورقية للتوضيح (صورة **9**).

ميزة استخدام جهاز الحاسوب المحمول هو استخدام خرائط عالية الدقة وذات أحجام كبيرة لا يستطيع الجهاز المصغّر اليدوي (**handheld GPS**) أن يحملها. ولإعطاء مثال على ذلك يكفي أن نعرف أن الجيش الأمريكي في عرباته المدرعة من نوع "هامفي *" يستخدم أجهزة حاسوب محمول مجهز بنظام مزدوج: جي بي إس و جي آي إس، كما يستخدم أجهــزة مدمجــة و محمية داخل العربات، حيث تحتاج إلى وقت لنزعها من العربات، و هذا الوقت غير متاح في حالة العمليــات الــتي تحتــاج لانسحاب فوري (صورة **11-12**).





صورة 8 : بطاقة جي بي إس للحاسوب المحمول



صورة 9: استخدام جي بي آس يدوي مع الاستعانة بخارطة خارجية



صورة 10 : جهاز حاسوب خاص بالجيش مع نظام تحديد الموقع مدمج و مجهز ببرنامج معلومات جغرافي من مايكروسوفت **(Streetpilot)**





صورة 11 : جهاز تحديد الموقع مدمج داخل عربة عسكرية (هامفي). لاحظوا الأقفال الموجودة لحماية الجهاز. انتبه! هناك تحذير داخل المربع الأحمر (يبدو أن شيئا خطيرا مرتبط بهذا التحذير...!)



صورة 12 : حماية جهاز تحديد الموقع المدمج داخل عربة عسكرية (هامفي) لمنع المجاهدين من الحصول عليه بسهولة. نزع الأقفال والحماية يتطلب وقتا غير متاح أثناء العمليات. (حذر شديد في ما هو مرتبط به....!)

5. عمل مستقبلي:

في المقال القادم إن شاء الله سوف نشرح كيف يتم تعطيل أجهزة الجي بي إس، ومنع الجيش من معرفة موقع آلياته على الأرض، و بالتالي تأخير وصول النجدة في حالة تعرضهم لهجوم.

اللهم علمنا ما ينفعنا و إنفع إمتنا بما علمتنا

و السلام عليكم و رحمة الله و بركاته.

{وَجَعَلْنَا مِن بَيْنِ أَيْدِيهِمْ سَدًّا وَمِنْ خَلْفِهِمْ سَدًّا فَأَغْشَيْنَاهُمْ فَهُمْ لاَ يُبْصِرُونَ}



كيف تحمي ملفاتك حتى لو تم اختراق جهازك

بقلم : أبو إسامة الشامي



رغم كل إجراءات الأمن والحماية ، إلا أن الإنسان دوماً معرض لمشاكل الاختراق ، فلربما يقع الأخ في خطأ يمكن أذناب الصليب من اختراق جهازه ، فما الذي يمكن للمجاهدين و أنصارهم فعله تحسباً لمثل هذه اللحظة ؟؟ هذا هو موضوع مقالتنا هذه.

حينما يكون جهازك متصلاً بالإنترنت فجهازك معرض لأي أسلوب من أساليب الاختراق الكثيرة، وفي حال تم هذا – لا سمح الله– فقد يمكن الوصول إلى بياناتك ومعلوماتك الشخصية التي قد تؤدي إلى الإضرار بك –لا سمح الله– ، فهل من حل؟؟

الحقيقة أن أفضل حل هو تخصيص جهازين ، أحدهما فقط للإنترنت والآخر تخزن عليه ملفاتك الشخصية ، ولكن مشكلة هذا الحل أنه غير عملي ومكلف ، فهل من بديل ؟؟

أقول نعم ! البديل هو برنامج الجهاز الظاهري **vmware** ...

ما هو هذا البرنامج و ما طبيعة عمله ؟؟

الحقيقة أن للبرنامج الكثير الكثير من المميزات ، نأخذ منه ما ينفع الجهاد و أهله ، فعلى الله توكلنا وبسم الله بدأنا.

إن وظيفة هذا البرنامج هي إنشاء مساحة في الذاكرة وعلى القرص (ظاهرية) أي غير حقيقية **virtual** ، هذه المساحة تحتوي

على نظام تشغيل آخر مستقل تماماً عن النظام الأصلي المستضيف له ! ويمكنك تكبير الشاشة وكأنك بالفعل تعمل على جهاز آخر وقرص آخر باستخدام هذا البرنامج !!

يمكن أن تقوم بتنصيب الوندوز على جهازك بشكل طبيعي ، ولكن لا تقم ببرمجته ليعمل الإنترنت عليه ، ثم تقوم بتنزيل برنامج **vmware** الذي سيأخذ مساحة أنت تحددها له من القرص الصلب ، ومساحة أنت تحددها من الذاكرة (يفضل ألا تقل الذاكرة عندك عن **512** كي تستطيع قسمتها بشكل لا يضعف أداء الجهاز، ثم تقوم بتنصيب وندوز آخر جديد على المساحة الجديدة ، ولن يكون هناك إمكانية للوصول إلى الوندوز الأصلي من الوندوز الظاهري ! حيث لا يرى الجهاز الأصلي وكأن لا علاقة له به ! ولو احتجت نقل الملفات بينهما ستحتاج إلى عمل شبكة محلية ومشاركة ملفات !!

المهم بعد إنجاز ما سبق ، تستطيع برمجة الجهاز الظاهري ليعمل على الإنترنت ، و لو حدث وأن اختُرِق –لا سمح الله– فلن يمكن لأحد الوصول للجهاز الأصلي أو ملفاته ، و بهذا تعمل وكأن لديك جهازين ، بل و أكثر من ذلك : تستطيع أن تخفي ملف الـ **vmware** عن طريق الروت كيت (كما ورد في مقالة أخينا أبو طلحة المسلم حول فن إخفاء الملفات) ومن ثم تنتقل بجهازك بدون مشاكل فلو جلس أحدهم عليه وبحث فيه فلن يجد شيئاً مريباً..

والآن معاً كي نرى سوياً كيف يمكن فعل ذلك بالصور:



أولاً نقوم بتنصيب البرنامج ، هذه قائمة ببعض السيريالات لإصداراته المختلفة :

الإصدار **4** على اللنكس : **DRMA1-UW7A4-AAMFF-4YWX3**

الإصدار 4 على الوندوز : **KN-06NDD-4854F-4MDQ7590**

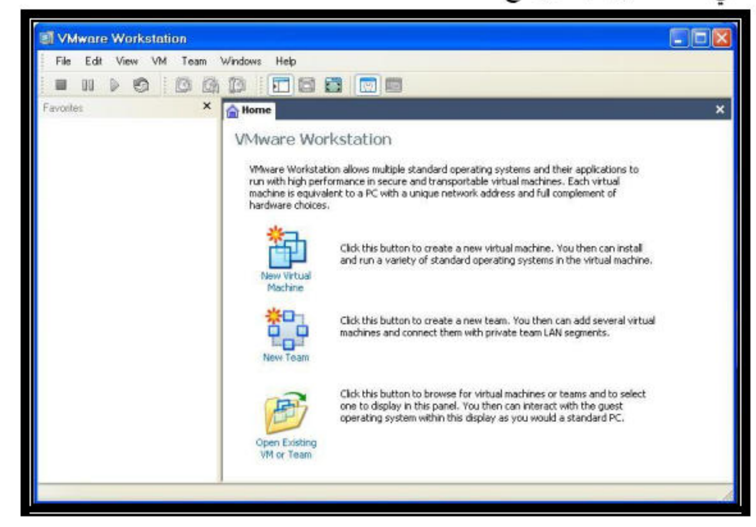
الإصدار 5 على الوندوز (تعمل هذه السيريالات حتى الإصدار 5.5) :

DTHR4-0WWFA-28H4U-4MRZ2

الإصدار 5 على اللنكس (تعمل هذه السيريالات حتى الإصدار 5.5) :

MLRAD-XH56L-P8M4A-4YRQP

بعد التنصيب هذه هي الشاشة الرئيسية للبرنامج :

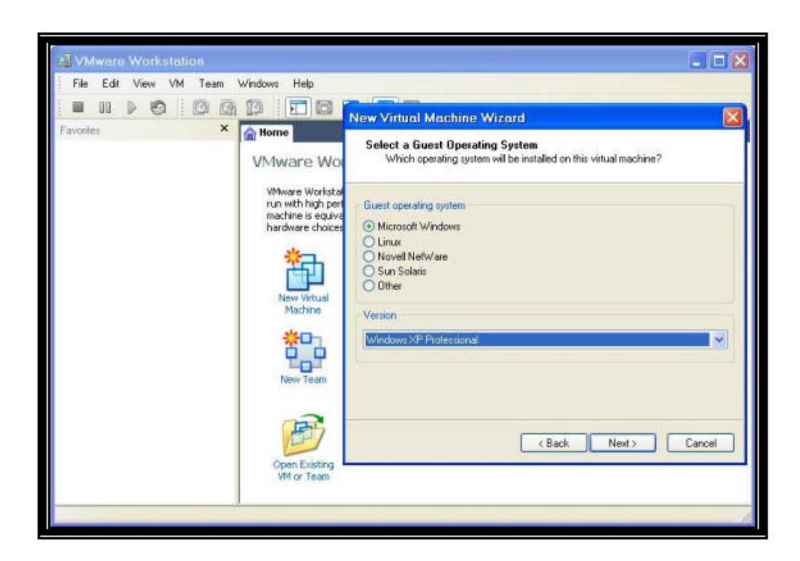


نقوم بإنشاء نظام جديد عن طريق الضغط على **New Virtual Machine** ، ثم نختار **Typical** ..

ملاحظة : يجب أن تكون اسطوانات النظام الذي تريد تنصيبه جاهزة الآن لديك لأنك ستحتاجها خلال لحظات ..

الآن نختار من الشاشة التالية نظام التشغيل الذي نريد تنصيبه ، وكما هو واضح المدى واسع للغاية ،يمكن تنصيب أي نظام تشغيل موجود في هذه الشاشة ، فقط علينا اختيار النظام والإصدار المناسبين لأن لكل نظام متطلبات يعمل النظام على

توفيرها ..



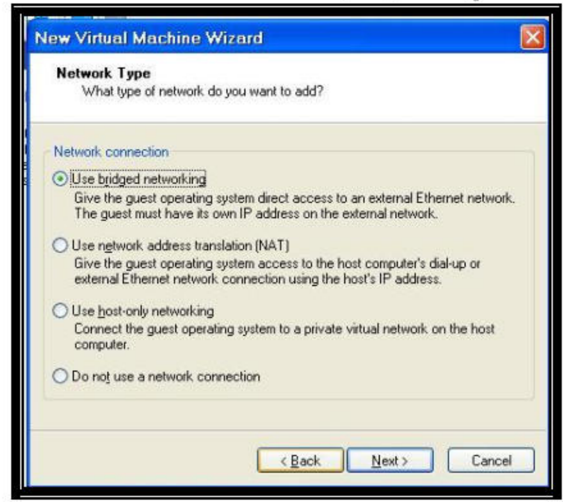
ثم نضغط التالي ..

في الشاشة التالية لاختيار النظام سيكون علينا اختيار ماذا نريد أن نسمي النظام ، بالإضافة إلى تحديد المسار المناسب الذي يحوي مساحة كافية ..

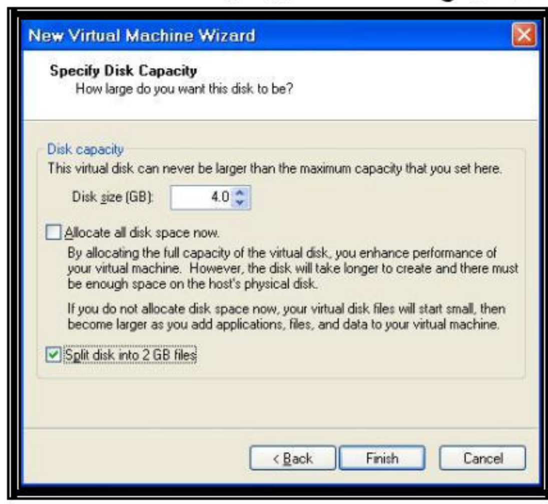




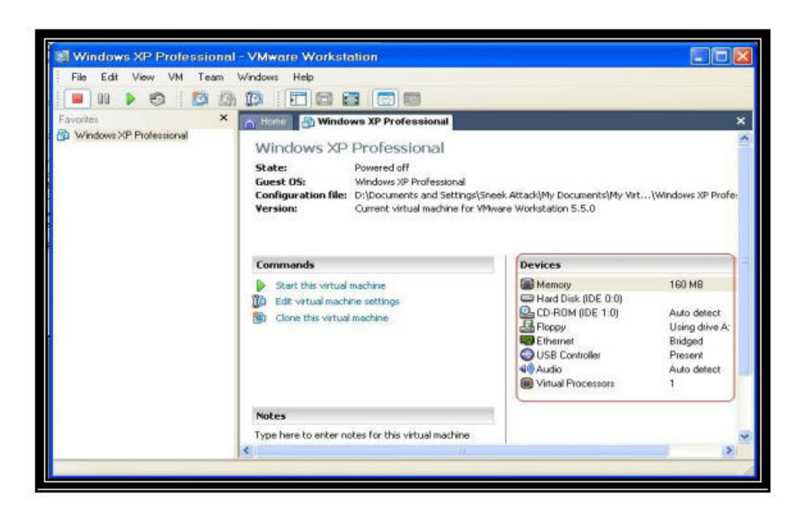
الآن نختار نظام الشبكة ، لدينا خيارين ، لكني دوماً أفضل الخيار الأول ، وهو ربط النظام الجديد مباشرة بكــرت الــشبكة (ملاحظة : عند اختيار هذا الخيار سيحصل النظام الجديد على **MAC Address** ظاهري / وهمي جديد ومختلف كليــاً عن الــ **MAC Address** الحقيقي! – للعلم فقط)



الآن نقوم باختيار مساحة الملف القصوى التي سيمكن للنظام الحصول عليها ، مع ملاحظة أن هذه المساحة ستبدو في النظـــام كقرص صلب ، وفرمتته من داخل البرنامج vmware لا تؤثر على ملفاتك ..

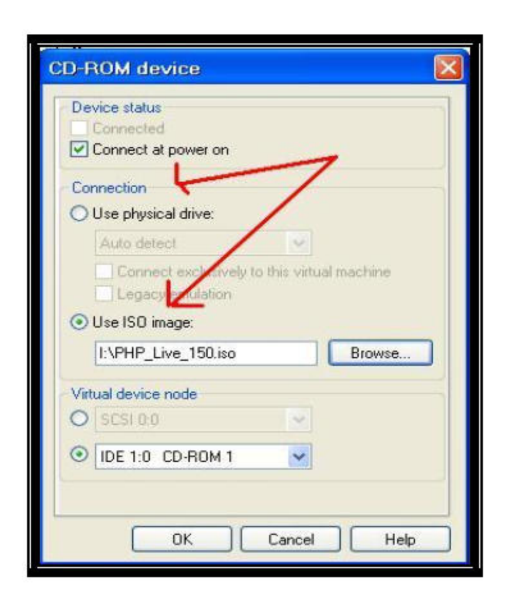


بعد الانتهاء الآن ، نقوم من المنطقة التالية بضبط الإعدادات الخاصة بالجهاز:



كما ترون ، الذاكرة و الأجهزة المختلفة نستطيع ضبطها من هنا ، كم مثلاً ستكون حصة النظام الظاهري من الذاكرة ، فلو كان مجموع الذاكرة عندك هو **512** ميغا ، فيمكن لك قسمتها إلى قسمين متساويين ، أو مثلاً : **340 – 172** ، وعموماً يفضل أن تكون الحصة الأكبر للنظام الأصلي ...

هناك أيضاً ، محرك الأقراص **CD-ROM** ، ويمكن لك اختيار من أي يبدأ التشغيل ، سواء كانت البداية **BOOT** من أحد محركات الأقراص في جهازك أو حتى من ملف **iso** ! و هذه ميزة مهمة و مفيدة .

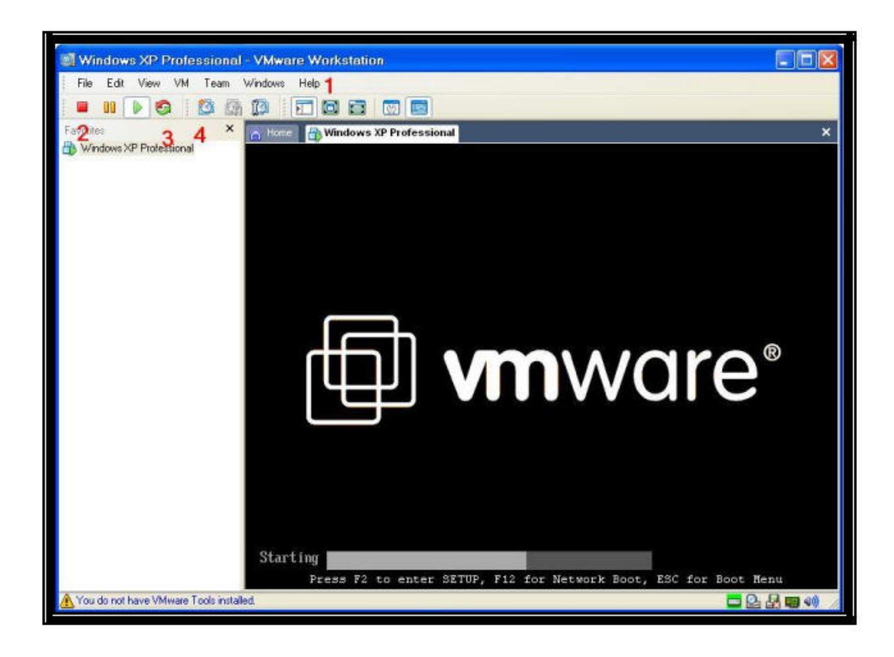


هل كل شيء جاهز ؟؟ أسطوانة نظام التشغيل موجودة داخل الجهاز ؟ إذن لنبدأ !

اضغط على : **Start this virtual machine**



سوف يبدأ النظام الجديد بالعمل ، كما في الصورة التالية :



الأزرار المرقمة :

1- العمل في وضع (ملء الشاشة – **fullscreen**)

2-إيقاف نظام التشغيل عن العمل

3- إعادة التشغيل – **reset**

4- **SnapShot** (حفظ وضع النظام أثناء لحظة معينة بحيث يمكن الرجوع لها فيما بعد ، طبعاً ستفقد أي تغييرات أجريتها بعد أي لقطة في حال عدت إليها)

في حال كنت تريد تعديل شيء من اللوحة الأم – البيوس – في الجهاز الجديد يمكنك أن تضغط **F2** في بداية تشغيل الجهاز !



إلى الجهاز الرئيسي يلزمك ضغط **CTRL+ALT** ، و لو احتجت أن تضغط **ctrl + alt + delete** داخل النظام الظاهري فاستبدل **delete** بزر **insert** ..

و الآن يمكنك البدء بعملية التنصيب بشكل طبيعي.

وفقنا الله وإياكم لما يحب ويرضى وبارك الله فيكم وحفظكم بعينه التي لا تنام



سلسلة شرح الفيديو (سؤال وجواب)

بقلم : مجاهد إعلامي



سنبدأ هنا بما يشبه دورة حول ما يخص مسائل الفيديو..

معظمنا يرى يومياً ملفات الفيديو ذات الامتدادات المختلفة ، ولعل بعضنا قد تساءل عن الفرق بين هذه الملفات .. يعني نجد مثلاً نفس الفلم مرة بامتداد **wmv** ومرة بامتداد **rm** ومرة بامتداد **rmvb** وغيرها الكثير .. وبعضنا قد يتساءل عن الفرق بين هذه الصيغ وما فائدة وجودها ولماذا لا يتم إيجاد صيغة موحدة تجمع بينها .. بعضنا الآخر يسمع عن وجود برامج تحويل بين هذه الصيغ ..

ومن يمارس التصوير الفيديوي على كاميرات الفيديو العادية ، ثم يحب أن ينسخ الفلم إلى **CD** أو **DVD** فلا بد أنه قد واجه مشكلة أن جهازه مثلاً لا يستطيع أن ينجز له ما يريد وإنما يحتاج إلى ما يسمى ببطاقة الفيديو (أو بطاقة الالتقاط) ، فيذهب مثلاً إلى من يملك مثل هذه البطاقة لينسخ له الفلم على **CD** .. طيب لم كل هذا العناء ؟ ولماذا الحاجة إلى بطاقة التقاط ؟

والكثير غير هذه المسائل التي واجهت الكثير منا .. سيتم طرحها هنا في هذا الموضوع ومناقشتها بشكل منهجي للوصول في النهاية إلى معرفة شاملة بإذن الله بما يخص الفيديو من معلومات تلزمنا.

ولنبدأ على بركة الله ..

أول سؤال خطر ببالي عندما بدأت أبحث عن مواد لتعلم هذا الفن هو



وما فائدة تعلم ذلك من الأساس ؟

ما الغاية من التحويل بين صيغ الفيديو ولم ينبغي تعلمها ؟ ما فائدة ذلك حقاً ؟

لم لا يتم الإبقاء على الصيغة الأساسية التي يتم التقاطها عن طريق كاميرا الفيديو ، ما عيب هذه الصيغة ؟ طيب وإن كان فيها عيب لم لا يتم تحويلها إلى صيغة أخرى فقط ؟ لم كل هذا الكم من الصيغ ؟

وقادني السؤال الأخير إلى:

وما هي الصيغة الأصلية التي يتم التقاطها عن طريق كاميرا الفيديو ؟ لنفرض الآن أن لدي كاميرا فيديو وأردت تسجيل مقطع مرئي لزيد ، طيب بعد الانتهاء من تسجيل هذا المقطع ما هي صيغة هذا المقطع الذي لدي ؟ ولم العناء في تحويلها ؟

أجابني أحد الإخوة قائلاً : فائدة هذا الفن أن الفيديو يعد من أهم وسائل نشر جهد إخواننا المجاهدين ، كما أنه من أهم وسائل التأثير. و لو قامت أحد المؤسسات الاعلامية الجهادية بإخراج 10 مقالات فإن تأثيرها في المستمع العادي قد لا يعادل تأثير فلم فيديو واحد.

الهدف الأساسي لهذا العلم يتلخص في الجملة التالية "أعلى وضوح بأقل حجم " ، وهناك العديد من صيغ الفيديو المملوكة لشركات, وهذه الشركات تتنافس في عمل أفضل أنواع الصيغ التي تحقق هذا الهدف ، و أكبر مثال على ذلك التنافس بين شركة **real** و شركة مايكروسوفت على إنتاج أفضل صيغة وهما **rm** و**wmv** ، أضف إلى ذلك أنه ظهرت في الآونة الأخيرة صيغ أخرى للفيديو منشؤها هم مجموعات من الأفراد المهتمين في هذا المجال مثل **divx** و **xvid** . وهذه بالإضافة إلى سعيها للهدف الأساسي وهو "أعلى وضوح بأقل حجم ممكن" فإنها أضافت إلى هذه المعادلة "و أكثر ميزات ممكنة" .. فظهرت لنا ميزة الترجمة **subtitle** ، وفي هذه الميزة فإن كل ما عليك عمله لترجمة فلم من أفلام المجاهدين هو أن تقوم بإضافة ملف صغير جداً يحتوي على الترجمة في نفس مجلد الفيلم و من ثم يظهر لك الفيلم و فيه الترجمة وكأن الترجمة قام بعملها و تنسيقها شركة محترفة للغاية. وهذه الميزة مهمة جداً لأشرطة المجاهدين و شيوخ الجهاد, حيث أنه يمكن بعد عمل الشريط أن تتم ترجمته إلى 10 لغات ويتم نشره على نطاق واسع.



وبالنسبة لسؤالك عن سبب عدم الإبقاء على الصيغة الأساسية التي يتم التقاطها عن طريق كاميرا الفيديو : المشكلة الأساسية في الصيغ التي يتم التقاطها مباشرة هي الحجم الهائل للملف ، ولتوضيح الأمر لك أكثر أخي : فان فيلماً مدتـه **10** دقـائق بدون ضغط (الصيغة الأم) فإن حجمه قد يتعدى **10** جيجا أحياناً ، وهذا الحجم الهائل يجعل من الفيلم غير قابل للاستعمال مطلقاً على الإنترنت.

بالطبع لقد تطورت تقنيات التقاط الفيديو وهي الآن تقوم بعمل ضغط جيد ، ولكنه من المستحيل أن يصل إلى درجة الضغط التي توفرها الصيغ الأخرى، لذلك نحن دائماً بحاجة إلى تحويل صيغة ما يتم التقاطه بالكاميرا إلى صيغة أخرى حتى يتم تـوفير المساحة ونصبح قادرين على وضعه على سي دي مثلاً أو نشره على الإنترنت.

و بالنسبة لعدد الصيغ فإنه لكثرة الشركات و المنظمات التي تعمل في هذا المجال فقد تجد أن الفروق بين بعضها قليلة جداً من ناحية الأداء ولكنها تختلف في أنها مجانية أو لا ، وقد تكون الفروق في الميزات الإضافية ، وقد تكـون الفـروق في درجـة الوضوح و الضغط و نحو ذلك.

طيب السؤال التالي سيكون:

أنا قمت بتسجيل مقطع فيديو باستخدام كاميرا فيديو (عادية) أو مثلاً قمت بتسجيل حلقة من برنامج تلفزيوني على مسجل فيديو من التلفاز ، كيف أقوم بنقل هذه المادة المرئية إلى الحاسوب حتى يمكنني نشرها ؟

سأجيب عن هذا السؤال عن طريق ترجمة عدة مقالات تتحدث عن هذا الأمر بالتفصيل ..

ففي هذا الدليل سنتعلم كيفية التقاط (**capture**) مادة فيديوية غير رقمية (**analog**) إلى الحاسـوب ، وسـنتعلم نمـط المعالجة اللاحقة التي ينبغي أن تطبق للحصول على جودة مقبولة .

مصدر المادة المرئية التي نريد معالجتها سيكون : نظام **PAL** أو **NTSC** (أي نظام تلفزيوني غير رقمي) ، وسـننتهي مـن المعالجة وبين أيدنا ملف فيديو بإحدى صيغ (**FFVFW , XviD , DivX3 , DivX5**) إن كنا نريد أن نشغل المادة المرئية على الحاسوب .. أو سننتهي بصيغة (**DVD , SVCD , CVD , VCD**) إن كان هدفنا تشغيل المادة المرئيـة



على مشغل دي في دي **DVD** مستقل . (أي أن الصيغة النهائية التي نريد الوصول إليها ستعتمد على الجهاز الذي ننـــوي تشغيل المادة الفيديوية عليه .. إما حاسوب أو مشغل دي في دي مستقل)

حسنٌ قبل أن نكمل ، ما معنى الالتقاط **Capturing** ؟؟

الالتقاط هنا (التقاط الفيديو) نقصد به دجتلة المادة التلفزيونية ، أي بمعنى أبسط تحويل المادة المرئية التلفزيونية غير الرقميـــة (**Analog**) إلى مادة رقمية (**Digital**) ..

طيب ولم نحتاج إلى هذا التحويل ؟

ببساطة يا صديقي العزيز نحن كل ما نفعله الآن هو ترجمة هذه المادة غير الرقمية إلى لغة الحاسوب حتى يفهمها ويفهم علينا ما نريد أن يفعله بها ..

وكيف سأقوم بتوصيل هذه المادة إلى حاسوبي ؟

ستحتاج يا صديقي إلى مدخل فيديو بالطبع .. هذا المدخل إما أن يكون هو مدخل الفيديو الخاص بجهاز التقاط التلفزيـــون في جهازك ، أو أن يكون هو مدخل الفيديو الخاص بكرت الجرافيكس (مثل **ASUS Delux**) الموجودة أيضاً في جهـــازك .. مع العلم أن الثاني أفضل من ناحية الإشارة **signal**.

حسنٌ أكمل وآسف على المقاطعة .. ☺

حسنٌ ، البرامج المستخدمة في التقاط الفيديو هي (على سبيل المثال) : **VirtualDub** ، و**VirtualVCR** . وهي تتيح لك الحصول على نتائج أفضل من النتائج التي ستحصل عليها من برنامج التقاط **mpeg2** الذي يأتي مع بطاقة الالتقاط .

سنفصل في الشرح هنا بين مهمتي التقاط وتخزين الفيديو ، وهذا يعني أنك في البداية تخزن المادة المرئية (متضمنةً الإعلانـــات والأمور الأخرى التي تريد حذفها) على القرص الصلب الخاص بك، والتخزين سيكون في البداية بالطبع دون ضغط للمادة . ثم في المرحلة الثانية سيأتي موضوع المعالجة والتحويل إلى الصيغة التي تريد .. تمام ؟



المعالجة اللاحقة للفيديو الملتقط سيتم شرحها بطريقتين مختلفتين : طريقة سهلة باستخدام الـ VirtualDub ، وطريقة متقدمة أكثر باستخدام AviSynth . (أرجو من القارئ المبتدئ مثلي أن ينسى ما أقوله هنا عن خطة البحث والشرح حتى لا نضيع، فلا داعي للرعب منذ الآن ، عندما نصل إلى هذه المفردات نحاول فهمها إن شاء الله ، ولكنني أكتبها كما هي من أجل دقة الترجمة)

الآن ، قبل أن نبدأ بالالتقاط علينا أن نتخذ قرارين مهمين من البداية : ما هي الصيغة الأخيرة التي ننوي الوصول إليها (كما قلت في بداية المقالة) ، وما هو كوديك الالتقاط capturing codec الذي تريد استخدامه .

1- الصيغة الأخيرة المبتغاة:

ما هي الصيغة التي تريدها ؟ هذا يعتمد بشكل خاص على طريقة عرض المادة المرئية ، هل تريد عرضها على الحاسوب ؟ فنقترح عليك إذن صيغة DivX3 أو FFVFW أو DivX5/XviD . وهذه الكوديكات codecs ستمكنك من تخزين الفيديو بجودة عالية جداً ومساحة صغيرة نسبياً (على CD أو قرص صلب). أم أنك تريد عرض المادة باستخدام مشغل دي في دي مستقل (والذي يستطيع أن يشغل mpeg1 (VCD) و mpeg2 (DVD, SVCD or CVD)) مع العلم أن بعض مشغلات الدي في دي المستقلة يمكنها تشغيل ملفات DivX ، وبعضها لا يمكنها حتى تشغيل SVCD . (أرجو أن تعتبر الجملة الأخيرة غير موجودة .. كتبت فقط للمتقدمين).

2- كوديك الالتقاط Capture codec :

في الأساس ينبغي أن يكون التقاطك للفيديو دون أي ضياع من مادته (قدر الإمكان) . لذلك فهناك نوعان من الكوديكات سيتم شرحهما : الـ Huffyuv codec والـ PicVideo MJPEG codec .

الفرق بينهما ببساطة هو أن الـ Huffyuv يعطي الجودة الأفضل ، ولكنه يحتاج في نفس الوقت إلى مساحة هائلة كذلك (ستحتاج تقريباً إلى 20 – 40 جيغابايت لساعة فيديو بحجم كامل ، ولكن الأخبار السعيدة عن هذا الكوديك هو أنه مجاني . الاختيار الثاني سيكون هو PicVideo MJPEG ، وهو يتميز عن سابقه بأنه يمكنك فيه أن تضبط جودة الترميز encoding quality ، فإذا اخترت ضبط هذه الجودة للمستوى الأعلى (20) فإن حجم الملف الناتج يمكن أن يصبح بحجم الملف الناتج عن Huffyuv ، ولكن يمكنك أن تسهل حياتك كثيراً بأن تختار مستوى جودة 19 أو 18 (بدلاً من 20 العليا) بحيث أنه ينقص حجم ملف الفيديو الناتج كثيراً بدون أن تؤثر كثيراً على جودة الفيديو . وبالطبع كلنا بانتظار



سماع النقاط السلبية لهذا الـ **PicVideo** ، وها هي : أولاً أن الصورة الناتجة عنه تكون أقل حدةً (**less sharp**) من صورة الأخ **Huffyuv** ، والأمر الثاني أن الـ **PicVideo** ليس مجانياً ، فعليك أن تدفع يا حبيب!!

فقط بسرعة لنتذكر خلاصة ما تحدثنا عنه حتى الآن : تحدثنا عن معنى الالتقاط وسببه ، ثم ذكرنا البرامج المستخدمة في الالتقاط (**VirtualDub** ، و**VirtualVCR**) والبرامج المستخدمة في معالجة ما التقطناه (**VirtualDub** و **AviSynth**) ، ثم قلنا أن طريقة المعالجة تعتمد على عاملين : (كيف نريد أن نشغل المادة النهائية (حاسوب أو مشغل **DVD**) ونوع الكوديك الذي سنستخدمه في الالتقاط (أيضاً نوعان)) .
وفقط ، كل الكلام السابق الممل لم يخرج عن هذه النقاط ، وكل ما تم ذكره من صيغ وغيرها لا يهمنا كثيراً في هذه اللحظة ما هي بالتحديد ، وعندما يأتي وقتها سيتم التحدث عنها بالتفصيل إن شاء الله ..

قبل أن أستكمل الحديث أريد أن أوضح معنى كوديك **codec** .. ببساطة هو عبارة عن برنامج أو جهاز يقوم بعملية ترميز + فك ترميز (**coding + decoding**) واسمه خرج من جمع الحروف التي تحتها خط في الجملة السابقة ، فهو إذن برنامج يقوم بالترميز من صيغة (س) إلى صيغة (ص) ويمكنه فك الترميز والعودة من صيغة (ص) إلى صيغة (س) .. واسمه يختلف بحسب الصيغ التي أوكل إليه ترميزها وفك ترميزها .. إذن فالكوديك هو برنامج وظيفته أن يقوم بترميز صيغة (س) إلى صيغة (ص) وعكس الترميز من (ص) إلى (س) .. وفقط

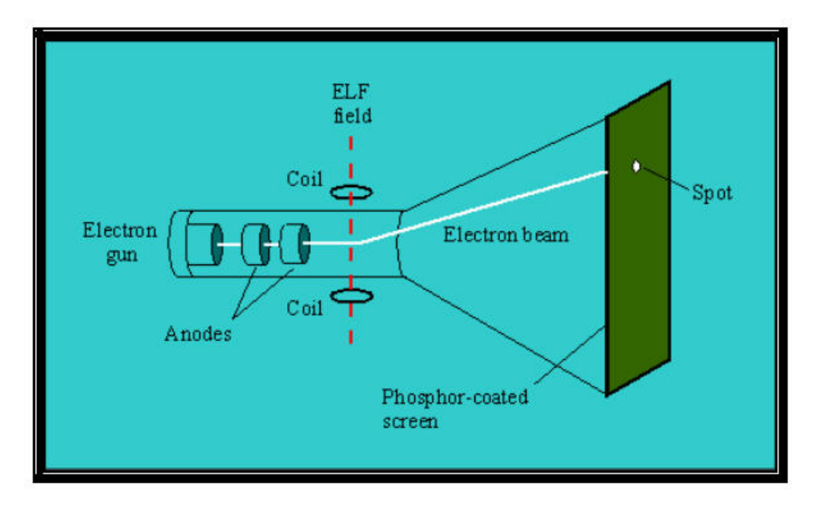
وقبل الولوج بموضوع الفيديو ، أليس من الأفضل أن نأخذ فكرة عن أساسياته الأساسية ؟ يعني لا بأس بمقدمة بسيطة (هي المقالة الموجودة هنا) عن طريقة عرض الصورة التي نراها على التلفاز .. وبعدها يصبح لدينا إلمام أكثر بالمادة التي سنجري عليها عملياتنا ..

سأبدأ بسؤال فضولي : كيف تظهر الصورة على التلفاز ؟

والجواب هو التالي :



أول ما تم اختراع التلفاز تم اختراعه على شكل أنبوب أشعة مهبطية (**cathode ray tube**) ، (يشبه الأنبوب الذي يصدر أشعة **X** المستخدمة في الطب) .. المهم لا داعي الآن لدورة فيزياء معقدة ولكن يمكننا ببساطة أن نقول ، هناك أنبوب ، تمام ؟ ، في أحد طرفيه (الطرف الخلفي) ما يسمى بـ "مدفع إلكتروني" وهو كما يظهر من اسمه مصدر لإطلاق إلكترونات (يحتاج بعض التسخين حتى يبدأ عمله ولذلك عند تشغيلك لتلفاز تلاحظ أنه يحتاج بعض ثوانٍ حتى يضيء) ، هذه الإلكترونات يتم توجيهها على طول هذا الأنبوب عن طريق حقول كهرطيسية ، وحسب توجيه هذه الإلكترونات فإنها في النهاية تسقط في النهاية الأخرى للأنبوب (النهاية الأمامية) على الشاشة المطلية بطبقة فوسفورية من الداخل ، عندما يصطدم هذا الإلكترون بهذه الطبقة فإنه يضيء منطقة الاصطدام .. هذه ببساطة كل القصة ، وطبعاً حسب توجيه الإلكترونات يتم رسم الصورة . وهذا مخطط سريع لما تحدثنا عنه هنا :



ولا تشغل نفسك أخي الحبيب بكل هذه التفاصيل فقط اعلم أن الخط الأبيض هو مسار الإلكترون والأخضر هو الطبقة الفوسفورية .

في البداية كانت أجهزة التلفاز أبيض وأسود لذلك كان يكفي لحزمة إلكترونات واحدة أن تؤدي مهمة رسم الصورة ، ولكن بعد ذلك خرجت التلفزيونات الملونة ، وصار يلزمنا أكثر من حزمة إلكترون في نفس الوقت لرسم تفاصيل الصورة لأنه صار عليها أن تمسح كامل الشاشة لتظهر كل التفاصيل .. الآن معدل مسح الشاشة هذا يصطلح على تسميته بـ "معدل الإنعاش"

(refresh rate) ، وهذا المعدل تم اختيار قيمته بناءً على مقدرة الأجهزة في ذلك الوقت .. ففي أمريكا الشمالية وأجزاء من اليابان تم اختيار معدل **60** هرتز ، وفي منطقة أوروبا والشرق الأوسط وأجزاء من آسيا تم اختيار معدل **50** هرتز ..

هذا الاختلاف أدى إلى نشوء نظامين متنافسين في أجهزة التلفزيون :

أولاً نظام الـ **NTSC** في الأماكن التي استخدمت الـ 60 هرتز .. ورقمياً هـذا النظـام كـان يرسـم (بواسـطة الإلكتـرون المسكين)**525** خطاً أفقياً (يظهر منهم **487**) ، ويرسم هذه الخطوط **60** مرة في الثانية (بناءً على معدل الإنعاش)

وثانياً نظام الـ **PAL** في الأماكن التي استخدمت الـ **50** هرتز .. ورقمياً يرسم هذا النظام (أيضاً بواسـطة الإلكتـرون) **625** خطاً أفقياً (يظهر منهم حوالي **540**) يتم رسمهم **50** مرة في الثانية (بناءً على معدل الإنعاش)

حسنا في ذلك الزمن لم تكن التقنية قد وصلت إلى إنتاج أجهزة رخيصة تستطيع أن ترسم هذا العدد الهائل مـن الخطـوط في الثانية (**525** خط يتم رسمهم **60** مرة في الثانية أي **31500** خط في الثانية ، وهو رقم كبير في ذلك الوقت) ، فلـو أرادوا ذلك لارتفع سعر التلفاز كثيراً مما يحد من استخدامه ، حـسنا إذن ماذا عن تخفيف معدل الإنعاش (بدل **60** أو **50** نجعلـها **40** أو **30**)؟ أيضاً هذا كان يحتاج إلى دارات معقدة ستؤدي أيضاً إلى رفع سعر التلفاز ، فضلاً عن أن تقليل معدل الإنعاش سيجعل العين البشرية تشعر بأن الصورة غير انسيابية (متقطعة) ، فهناك حد أدنى للعين البشرية لإدراك الانسيابية ..

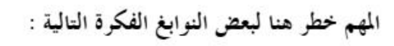
1 3 5 7 9 11

upper field

2 4 6 8 10 12

lower field

المهم خطر هنا لبعض النوابغ الفكرة التالية :



ماذا لو قمنا برسم كل ثاني خط بدلاً من رسم الخطوط المتتابعة خلال مسحة الشاشة الأولى ثم بعد الانتـهاء نعـود لنرسـم الخطوط التي تركناها وهكذا .. أي أن مسح جميـع خطـوط



حسناً أنا لم أفهم ما الغاية من هذا التعقيد ؟

الغاية أننا الآن صرنا عملياً ننتج معدل إنعاش (60 بدلاً من 30، و 50 بدلاً من 25) وفي نفس الوقت التففنا حول مسألة العين البشرية ومشاكلها ، فالمعدل الحقيقي الذي تراه العين هو 60 أو 50 (حسب النظام كما قلنا) ، ولكن عملياً كل إنعاشين من هذه الـ 60 أو الـ 50 هي لصورة واحدة ، أي كأننا نبث 60 أو 50 صورة بدلاً من بث 30 أو 25 صورة ، أي أن الأجهزة الرخيصة التي تستطيع رسم 525 خط 30 مرة في الثانية صارت تنفع لتعمل في التلفزيون (بدلاً من استخدام الأجهزة الغالية القادرة على رسم 525 خط 60 مرة في الثانية) ، وفي النهاية العين سترى الصورة نفسها ..

حسنا الآن بالصور لنر ما قصدناه ببساطة :

فهنا خلال المسحة الأولى كما نلاحظة تم مسح الخطوط 1 و 3 و 5 ... حتى نهاية الشاشة ، ثم بدأت المسحة الجديدة لترسم الخطوط 2 و 4 و 6 ... والمسحتان لنفس الصورة ..

حسناً ماذا نسمي الخطوط الناجمة عن إحدى المسحتين ؟

في المسحة الأولى نتجت خطوط فردية (أو زوجية) وهذه الخطوط بمجملها سنصطلح على تسميتها بالحقل (**field**) وهنا الحقل علوي (**upper field**) ، والمسحة الثانية أنتجت لنا خطوطاً زوجية ، وهي تمثل الحقل السفلي (**lower field**).

ومن يقوم بكل هذا العمل المضني ؟

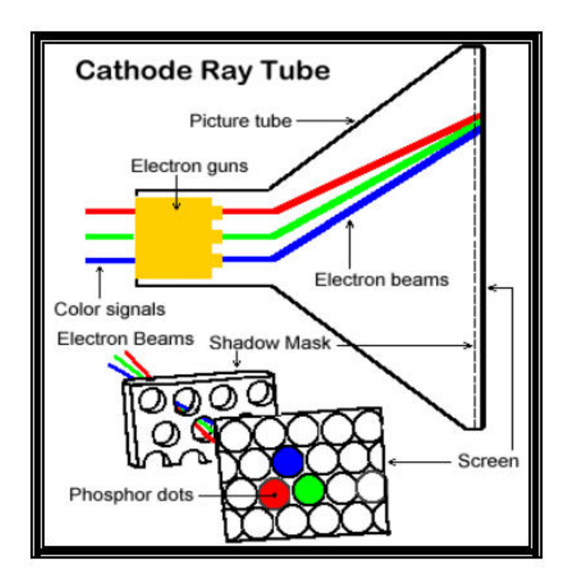
تقوم به حزمة الإلكترونات المسكينة ، والتي ما إن تنتهي من رسم الخطوط الفردية حتى تقفز إلى أول الشاشة من جديد لترسم الخطوط الزوجية ، ولا تحاول أخي أن تراقب شاشة التلفاز وتضيع وقتك في محاولة تصديق هذا الأمر ، فلن تلاحظ ذلك مهما حاولت التدقيق ، لأن طبقة الفوسفور تلك التي تطلي الشاشة من الداخل تبقى متوهجة من المسحة الأولى ريثما تصلها المسحة الثانية ، وبالتالي نحن البشر لن نلاحظ الفرق.



الآن مصطلح جديد : ما اسم عملية تقسيم الشاشة إلى حقلين كما تحدثنا الآن ؟

هذه العميلة اسمها بالعنجليزية: **interlacing** ، وأنا لم أجد أفضل من كلمة "تداخل" للتعبير عنها ، أعرف أنها ترجمة ركيكة ولكن هذا ما جادت به قريحة أخيكم ، وأظن أن المعنى أصبح واضحاً لدى الجميع فعندما نقول كلمة "تداخل" فإننا نعني كل هذا الكلام ، وطبعاً عملية إزالة هذا التداخل سنسميها ببساطة : "إزالة التداخل" **deinterlacing** .

للفضوليين فقط : عندما تم اختراع التلفزيون الملون بقيت تقنية التداخل هذه على حالها ، ولكن الجديد أنه صرنا بحاجة إلى أنبوب أشعة مهبطية أكثر تعقيداً ، فبدلاً من حزمة إلكترون واحدة (تظهر النقطة التي تسقط عليها إما أبيض أو أسود) صرنا نحتاج إلى 3 حزم إلكترونية ملونة كما في الشكل :



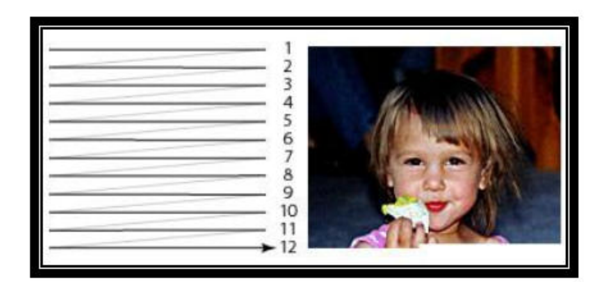
ألوان الحزم الثلاث المستخدمة هي: أحمر وأخضر وأزرق ، ولا يقل أحد لم لم يتم استخدام غيرها ، إن شاء الله فيما بعد سأشرح الموضوع كاملاً ، وسيكون موضوعاً ممتعاً جداً .. ، وأمر الألوان أيضاً فيه خداع للعين البشرية ، فعندما تكون 3 نقاط ملونة قريبة جداً من بعضها فإن العين تراها لوناً واحداً هو نتيجة مزج هذه الألوان الثلاثة حسب النسب ، وبالتالي يصبح موضوع إظهار اللون سهلاً يعتمد على تغيير نسب هذه الألوان الثلاثة ..

الآن كلمة مهمة جداً في المقدمة وهي أن :

شاشة التلفزيون مختلفة تماماً عن شاشة حاسوبك أخي الكريم ، فالتلفزيون كما قلت يتم فيه إظهار الصورة عن طريق تقنية التداخل **interlacing** لأنه عندما تم اختراعه كما قلت كانت أجهزة إنتاج معدلات الإنعاش العالية (**60** أو **50**) غالية وغير مناسبة لوضعها في أجهزة تلفاز ، أما الآن فأجهزة إنتاج معدلات الإنعاش هذه أصبحت رخيصة ، ولذلك لم نعد بحاجة إلى كل هذه المعمعة من أجل إخراج الصورة ، وكما تعلم شاشة الحاسوب تم اختراعها حديثاً وبالتالي تستخدم فيها هذه الأجهزة المتطورة ..

يعني ماذا تريد أن تقول ؟

أريد أن أقول أنه في شاشات حواسيبنا لا يوجد شيء اسمه تداخل **interlacing** وإنما يتم رسم الصورة ببساطة دون قفز فوق الخطوط أو شيء كما في الصورة :



حسناً وخيراً إن شاء الله أين المشكلة ؟

المشكلة أن المواد المرئية التي تعرض على التلفزيون لن يمكن عرضها على شاشتك يا عزيزي بسبب اختلاف طريقة العرض كما أسلفت ..

إذن ما الحل ؟

الحل هو إزالة التداخل **deinterlacing** الذي في صورة التلفزيون وتحويله إلى صورة غير متداخلة يمكن لشاشة الحاسوب عرضها .. وهذه هي إحدى خطوات المعالجة للمادة المرئية الملتقطة من التلفاز أو كاميرا الفيديو العادية غير الرقمية ..



وبكلمات أخرى فإن هناك عدة أمور ينبغي إجراؤها قبل عرض مادة تلفزيونية على شاشة الحاسوب ، وعملية إزالة التـداخل **deinterlacing** هي واحدة من هذه الخطوات ،

وكلمة صغيرة جداً حول لماذا قلنا في بداية المقالة أنه في الـ NTSC مثلاً يوجد 525 يظهر منها 487 ، وفي الـ PAL 625 يظهر منها 540 ؟

هذا بسبب الطبقة السوداء التي نعرفها جميعاً والموجودة حول إطار شاشة التلفزيون ، وسبب هذه الطبقة هو أنه كما نعلم معظم أجهزة التلفزيون (عدا الحديثة منها كالـ **LCD** والبلازما) معظم الأجهزة القديمة كانت غير مسطحة ، ورسم الصورة في النهاية العلوية للشاشة والنهاية السفلية ، وكذلك أقصى اليمين وأقصى اليسار كان يتسبب في حدوث زوغان للصورة (بسبب عدم وجود التسطح وصعوبة رسم الصورة في هذه الأماكن) ، لذلك تم وضع هذه المساحة السوداء في المحيط حتى لا يظهر الزوغان ، وهذا سبب غياب بعض الخطوط عن مجال الرؤية
الآن قبل أن أنهي المقالة أريد أن أتكلم شيئاً عن موضوع الإطارات ..

عندما كان يتم تصوير الأفلام السينمائية قديماً كان يتم ذلك على مواد كالتي نستخدمها في التصوير الفوتوغرافي التقليدي ، ولكن يتم التقاط هذه الصور بسرعة كبيرة (**24** صورة في الثانية) وعرضها بنفس السرعة الكبيرة بحيث أن عين المشاهد تنخدع ، فالعين في هذه الحالة لا ترى **24** صورة ثابتة متتابعة ، وإنما (بسبب سرعة عرض الصور) ترى أنه مشهد متحرك ، وهو في حقيقة الأمر صور ثابتة تعرض بسرعة وراء بعضها ..

فنظرياً لو أنك قمت أخي الكريم باستخدام كمرتك التصوير العادية (الفوتوغرافية) بتصوير مشهد ما وذلك بسرعة **24** لقطة في الثانية ثم قمت بعرضها بنفس السرعة فما ستشاهده هو مشهد متحرك ، طبعاً لن تستطيع ذلك لأنه سيلزمك في هذه الحالة أن تبدل أفلام التصوير كل ثانية أو كل ثانية ونصف .. المهم فكان يتم التقاط **24** صورة في الثانية ، ونحن عندما نشاهد الفلم في السينما فما نشاهده هو عبارة عن صور ثابتة (يصطلح على تسميتها بالإطارات ، فكل صورة هي إطار) يتم عرض هذه الصور أو الإطارات بسرعة **24** إطار في الثانية الواحدة ..

وكل هذا الكلام هو من أجل أن أخبرك بمعنى الإطار ، فهذا هو معناه : الصورة الثابتة التي يتم التقاطها بواسطة كاميرا الفيديو والتي يعرض منها **24** إطارا في الثانية في حالة الأفلام السينمائية .. أعتقد أن المعنى واضح جداً.



وأخيراً (لا تقلقوا لن أكمل هذه النقطة الآن) .. عدم التنسيق بين منتجي الأفلام السينمائية وبين مصنعي أجهزة التلفاز أدى إلى مشكلة جديدة : الأفلام يتم إنتاجها على شكل **24** إطار (أو صورة) في الثانية ، وشاشات عرض الـ **PAL** مصممة لعرض **25** صورة في الثانية (كما أسلفنا بعد تقنية التداخل نقصت من **50** إلى **25**) ، وشاشات الـ **NTSC** على أسوأ ، فهي تعرض **30** صورة في الثانية (للدقة الـ **NTSC** تعرض **29.94** صورة في الثانية وذلك بعد بعض التعديلات من أجل استيعاب النظام اللوني) ، المهم أننا إذا أردنا عرض الفلم السينمائي الذي كان يأتي على شكل شريط فيديو **VHS** (الفلم البلاستيكي الكبير الذي كان يستخدم قديماً قبل اختراع القرص المضغوط) ، أو الذي يأتي الآن على شكل قرص **CD** أو **DVD** فإنها سيحدث اختلاف بين معدل عرض الصور في الفلم وبين معدل عرض الصور على شاشة التلفزيون .. فكيف نحل هذه المشكلة ؟

سأؤجل الحديث عن هذه النقطة إلى مقالة قادمة بإذن الله ولكنني فقط أردت لفت النظر إلى هذه النقطة أيضاً .

والآن للتذكير ما نخرج به من كل هذا الكلام هو معرفة:

- مبدأ رسم الصورة التلفزيونية ببساطة
- معنى الخط
- معنى الحقل
- معنى "معدل الإنعاش" **refresh rate**
- معنى التداخل **interlacing** وإزالة التداخل **deinterlacing** وسبب الحاجة لهما
- ومعنى الإطار **frame** ، ومنه الواحدة **fps** وهي تعني **frame per second** ، أي (كذا) إطار في الثانية ، وهي واحدة ستمر معنا كثيراً (وهي في أفلام السينما مثلاً **24 fps**).

و الى اللقاء في الحلقة القادمة من السلسلة إن شاء الله



تعريف ببرنامج PGP وهل هو آمن بما فيه الكفاية للمجاهدين؟

بقلم : أبو مصعب الجزائري

1. حول الشركة:

شركة بي جي بي أسسها شخص اسمه فيليب زيمرمن (**Philip Zimmerman**) في بداية التسعينات، وقامت الشركة بتوقيع ببرمجة خوارزمية **RSA** للمفاتيح اللامتناضرة (**anti-symmetric**) و إنتاج برنامج مع كود مفتوح وهذا ما أثار حفيظة الحكومة الأمريكية فقامت الحكومة مع شركة (**RSA security**) برفع قضية أمام المحكمة العليا لتوقيف إنتاج هذا البرنامج اعتماداً على أن خوارزمية **RSA** محمية ببراءة اختراع لصالح **RSA security**. و شركة **PGP** دافعت عن نفسها على أساس أنها وقعت عقداً مع شركة ثالثة تمتلك حقوق استخدام خوارزمية مفاتيح **RSA**. دام الجدال طويلاً و في **1999** تم توقيع اتفاقية بين الحكومة الأمريكية وشركة **RSA security** من جهة و شركة **PGP** من جهة أخرى. و بموجب هته الاتفاقية التي لا نعرف جميع بنودها تقوم شركة بي جي بي بإلغاء استخدام مفاتيح **RSA** من برنامجها وتستخدم مفاتيح **ELG** و **DSS (DSA)**. وتمتنع عن كشف الكود المصدر من البرنامج للنسخة التجارية. ومقابل هذا تم إلغاء جميع الدعاوى القضائية ضد الشركة.

2. البرنامج:

يقول خبراء أمن المعلومات إن برنامج **PGP** تدور حوله الكثير من الشكوك بعد الاتفاقية الموقعة مع الحكومة الأمريكية وأن آخر نسخة آمنة هي النسخة **2.6** وما بعدها لا يعرف عنه شيء. وإن إلغاء استخدام مفاتيح **RSA** واستبدالها بمفاتيح **ELG** ربما هو مؤشر على ثغرات في البرنامج، خاصة وأن حقوق الملكية للمفاتيح **RSA** انتهت سنة **2000** ولا يوجد مبرر لعدم استخدام المفاتيح سوى كونها مفاتيح قوية لأنها تعتمد على الأعداد الأولية.



3. المفاتيح من نوع RSA:

المفاتيح تعتمد على خوارزمية رياضياتية تم اختراعها من قبل ثلاثة دكاترة هم (**Rivest, Shamir, Aldman**) وتعتمد على الأعداد الأولية (**prime numbers**)، وقد تم كسر مفتاح **512** بت في مدة **18** شهراً، ويعتقد (في سنة **2000**) أن مفتاح **1024** بت يستغرق كسره **52** مليون سنة بمواصفات حواسيب **2000** ، وهذا إذا لم يتم اكتشاف طريقة رياضياتية لتحليل الأعداد الأولية التي تدخل في إنتاج المفاتيح. ويعتبر مفتاح **2048** آمناً لفترة تزيد عن عشر سنوات على أقل تقدير. (على اعتبار أن أي اكتشاف علمي مهم يستغرق أكثر من عشر سنوات من الأبحاث) وعلماً بأن الأعداد الأولية التي تدخل في إنتاج المفاتيح تعتبر لغزاً في الرياضيات و لا توجد حالياً طريقة لحسابها، بل يتم إنتاجها بالتجربة فقط وليس اعتماداً على قوانين.

في التجارب التي قمت بها في إنتاج مفاتيح (ببرامج أخرى) فإن الأمر يتطلب عادةً ما بين **20** دقيقة و **50** دقيقة لإنتاج مفاتيح من **4096** بت، بينما يقوم برنامج بي جي بي بإنتاجها في ثواني معدودة. وهذا يدل أن المفاتيح لا تنتج فعلياً بطريقة عشوائية وإنما اعتماداً على (**Seed**)، والسييد هو تعريف بداية التسلسل في الأرقام الشبه عشوائية (**Pseudo random**) لأنه لا توجد هناك أرقام عشوائية بالمعنى النظري، وإنما شبه عشوائية. وإذا لم تكن تعرف السييد (**Seed**) فهذا يجعلك غير قادر على إعادة إنتاج الأرقام نفسها كل مرة، أما إذا اعتمدت على بدايات ثابتة فإنه بالإمكان إنتاج مفاتيح و إعادة إنتاجها مرة أخرى مما يلغي سرية المفاتيح، وهذا يعتبر أمرا كارثياً.
وقد تحققت من ذلك فقمت بإنتاج مفاتيح اعتماداً على تسلسل معين واستطعت إنتاج مفاتيح و تكرار إنتاجها في مرات مختلفة، وهنا يكمن الخطر!!!.

4. مفاتيح ELG

مفاتيح **ELG** نسبة للدكتور طاهر الجمل هي مفاتيح للتشفير اللامتناظر لها نفس هدف مفاتيح **RSA** ، وهذه المفاتيح تعتمد على الخوارزم المتقطع (**Discrete logarithms**) و يعتقد أنها أضعف من مفاتيح **RSA**. (سوف أقوم مستقبلاً بعمل دراسة حولها إن شاء الله).

5. برنامج PGP و تشفير القرص الصلب

التحذير التالي هو من شركة بي جي بي:

At the end of the trial period, any local disks that have been encrypted using PGP Whole Disk Encryption will **automatically decrypt**.

هذا أخطر ما في الموضوع، فكيف للبرنامج أن يقوم بفك التشفير تلقائياً!!

هذا يعني أن البرنامج يحتفظ بنسخة من المفتاح الخاص (**private**) ويقوم باستخدامها لفك التشفير. !!!

كيف تسمح الشركة (**PGP**) بالاحتفاظ بنسخة من المفتاح الخاص داخل البرنامج واستخدامها دون علمك؟! و هذا يعني أنه بالإمكان في حالات أخرى أن يتم إعطاء أمر للبرنامج ليقوم بفك تشفير القرص الصلب!.

تشفير القرص الصلب باستخدام **PGP** ليس له علاقة بالأمن الفعلي فهو مجرد خداع، فإذا كان البرنامج يستطيع فك التشفير تلقائياً (عند نهاية الفترة التجريبية) دون أن تعطيه المفتاح الخاص ودون أن تطلب منه ذلك؛ فإنه بإمكانه فعل نفس الشيء بأمر خاص من الشركة.! في أي وقت.

التشفير باستخدام هذه التقنية آمن للأمور الخاصة و التجارية ولكنه غير مناسب بالنسبة للأمور الجهادية. وذلك لأن شركة بي جي بي وقعت اتفاقية سرية مع الحكومة الأمريكية الله أعلم بما تحتويه.!

6. خلاصة:

وفقاً لماتوصلنا إليه حتى الآن نرى أنه ليس برنامجاً آمناً بالشكل المطلوب للشخصيات المهمة بناء على النسخة التي تم مراجعتها وجاري التثبت من هذا الأمر من قبل خبراء مجلتنا الغراء ويسعدنا تلقي رد من المتخصصين في هذا الأمر من قرائنا الكرام لتعم الفائدة.

دعوة للمشاركة

أخي المجاهد التقني يامن تقرأ كلامي هذا

السلام عليكم و رحمة الله و بركاته

كم مرة فكرت في خدمة هذا الدين و نصرة إخوانك المجاهدين إعلامياً ؟

هل تعتقد أن مجرد دخولك إلى المنتديات، والقراءة فيها فقط بدون عمل يعد خدمة لهذا الدين؟ متى ستنتقل أخي من مرحلة التلقي إلى مرحلة الإفادة؟

ألم يحن الوقت لأن تتفجر طاقاتك الكامنة ، وتصبح عضواً فاعلاً في الحرب الإعلامية بين المجاهدين وأعداء الله الصليبين؟

ألم تفكر يوماً أن لديك ما يمكن أن تنفع به إخوانك في دولة العراق الإسلامية الوليدة؟!!

أخي المجاهد التقني الكريم إن مجلة المجاهد التقني توفر لك هذه الفرصة ، فما تملكه من علمٍ أخي هو أمانة يتعين عليك إيصالها إلى غيرك من المجاهدين ورواد المنتديات، فهذه المجلة سيطلع عليها عشرات الآلاف من الأشخاص سواء من المجاهدين أو أنصارهم في المنتديات وعامة المسلمين فيحصل لك بمقالتك الأجر العظيم.

أخي المجاهد التقني إن معركتنا مع أعداء الله الذين احتلوا ديارنا في فلسطين وأفغانستان والعراق والشيشان يدور نصفها على الأقل في الإعلام وتوعية المسلمين بحقيقة هذه الحرب الصليبية على المسلمين ولقد كان هناك الكثير من النجاحات الهائلة للإعلام الجهادي التي شهد بها العدو قبل الصديق.

أخي المجاهد التقني بإمكانك اليوم البدء بإبداعاتك ومقالاتك العلمية التي تهم المجاهدين وأنصارهم من رواد المنتديات، ونحن نتكفل إن شاء الله بنشرها لكم في مجلتنا ، فيصلُ ما تكتبه إلى عشرات الآلاف من القراء من إخوانك المسلمين الذين هم الآن في أمس الحاجة لمثل هذه العلوم-وما نداء الشيخ أبي حمزة المهاجر حفظه الله عنا ببعيد-.

أخي المجاهد التقني الكريم ألم تسمع حديث رسول الله صلى الله عليه و سلم قال: ((إذَا مَاتَ الإنْسَانُ انْقطعَ عَمَلُه إلامِنْ ثلاثٍ :صَدَقةٍ جَارِيَةً ، وَعِلْمٍ يُنْتَفعُ بِه، وَوَلَدٍ صَالِحٍ يَدْعُو لَه).أفلا تحب أن يبقى عملك هذا بعد موتك؟

كما إننا في هيئة التحرير نتطلع إلى المزيد من التطوير والتحديث لأبواب المجلة من حيث الشكل والمضمون،إلا أننا مهما بلغنا من الحرص على ذلك فلا بد من حدوث بعض القصور فهذه طبيعة العمل البشري، فلذلك سنكون نحن أعضاء هيئة التحرير في غاية السعادة عندما نتلقى آراءكم واقتراحاتكم فيما يختص بتطوير المجلة شكلاً ومضمونا ، فنحن نرى فيكم عوناً لنا تمدوننا بالمشاركات، وعيناً لنا ترصدون أخطاءنا وتنيرون الطريق لنا.

كما أننا في هيئة التحرير ننتهز هذه الفرصة لدعوة جميع من يقرأ هذه المجلة من المسلمين إلى المشاركة معنا والمساهمة بمقالاتهم العلمية، حتى نرقى بمستوى هذه المجلة إلى المعالي بإذن الله.

إننا في القرن الحادي والعشرين فليس لنا مكاتب ثابتة أو بريد تقليدي بل مجلتنا هذه تنشر حصرياً على شبكة الإنترنت ولنا بريد إلكتروني خاص نستقبل عليه الرسائل وسيتم إيصالها لآلاف المشتركين وتنشر حصرياً في أهم المنتديات الجهادية في العالم وهي التي يتم النشر فيها حالياً من قبل مركز الفجر للإعلام الذي نعمل تحت لوائه

بقي أن نذكر أن مجلة المجاهد التقني تصدر عن مركز الفجرللاعلام (وهو المركز المكلف رسمياً بنشر بيانات عدد من الجماعات الجهادية في أنحاء العالم وعلى رأسها إخواننا في تنظيم القاعدة بأفغانستان وإخواننا في دولة العراق الإسلامية ببلاد الرافدين وغيرها من الجماعات الجهادية المباركة) ومجلتنا الطيبة هذه وجه من أوجه الاستجابة لدعوة الشيخ أبي حمزة المهاجرأمير تنظيم القاعدة في بلاد الرافدين حول دعوته للخبراء والمتعلمين لنصرة الدولة الإسلامية الوليدة في بلاد الرافدين.

وإننا ماضون في حربنا هذه مع أعداء الله فوق كل أرض وتحت كل سماء حتى تحرر جميع أراضي المسلمين من رجس اليهود المعتدين والصليبيين الحاقدين ويكون الدين كله لله ونرى راية الإسلام خفاقة في الأرض.

والله أكبر والعزة لله ولرسوله وللمؤمنين....

يسعدنا تلقي إستفساراتكم ورسائلكم على بريد المجلة
http://teqanymag.arabform.com

أخوكم / رئيس التحرير
أبوالمثنى النجدي

الورقة الأخيرة

نريده في عقر دارهم

بقلم : البراق / عضو المكتب الاعلامي للجيش الإسلامي



الحمد لله رب العالمين والصلاة والسلام على امام المجاهدين رسولنا الكريم صلى الله عليه وسلم ...

اما بعد فان الاعلام الجهادي في زمننا الحاضر بات ركنا رئيسيا في معركة الاسلام ضد الصليبين وملة الكفر فالذي يقدمه الاعلام من دعم ومساندة معنوية للمجاهد المرابط في ارض المعركة المشعبة الميادين والاساليب يدفع جميع العاملين فيه الى البحث المستمر عن كل ما من شأنه يكون مؤثرا وفعالا يعين المجاهد ويمده باسباب الثبات والتمكين والحاق الهزيمة بالعدو عسكريا ونفسيا.

ان الحاق الهزيمة النفسية بالعدو المهمة الاولى للاعلام الجهادي والتي هي اشد واسرع اثرا من استخدام السلاح الحربي فقد روي ان عبد الله بن رواحة كان يلقي شعرا في هجاء الاعداء في المسجد فأستنكر منه ذلك عمر بن الخطاب رضي الله عنه قائلا: بين يدي رسول الله وفي حرم الله تقول الشعر؟! فقال الرسول صلى الله عليه وسلم: خل عنه يا عمر فلهي: يعني القصيدة– اسرع فيهم من نضح النبل "وفي رواية" عنه ياعمر فوالذي نفسي بيده لكلامه اشد عليهم من وقع النبل "رواه الترمذي والنسائي".



Video distributed on the Internet and on DVDs sold in Baghdad credits a lone gunman with scores of sniper attacks on U.S. troops in Iraq. The shooter calls himself "Juba the Baghdad Sniper." (ABC News)



اذا فحقيقة الامر التي لا بد من الركون اليها هي ان الاعلام الجهادي بكل مفرداته بحاجة الى اناس مؤمنين بالقضية التي يقاتلون من اجلها بالكلمة و الصوت و الصورة وكل التفرعات الخارجة منها.. اناس على درجة عالية من الألمام بالتقنيات الاعلامية وخاصة على شبكة الانترنت ولان هذا الامر متشعب وبحاجة الى مساحات كبيرة من الدراسة والتأمل للوقوف على حيثيات المعركة الاعلامية التي تكون فيها المواجهة قاسية لامكان فيها الا للاقوياء فنيا وتقنيا وقبلها روحيا من اجل ذلك سأتوقف عند اسلوب عمل اعلامي ان تمكنا من النجاح فيه فان خيرا كثيرا سيكون بانتظارنا هذا الاسلوب الذي اقصده هو وجوب العمل بهمة على انشاء مواقع وروابط تعمل باللغات الاجنبية الرئيسية في العالم وخاصة "الانكليزية" فالملاحظ وجود شحة وتقصير في مثل هذه الروابط التي نريد من خلالها الوصول الى الاعداء وخاصة عوائل الجنود فالذي نعرفه ان ملة الكفر التي يحاربها المجاهدون في أرض الرافدين وافغانستان فيها الكثير من القوميات متعددة اللغات ولكي تمكن من ايصال ما يقوم به اسود الشرى بجنود الكفر الى عوائلهم فلابد ان ننشأ مواقع وروابط بلغات بلدانهم والاستفادة من اخوتنا المتمكنين في اللغات الاجنبية كلا حسب اختصاصه وتخيلوا لو اننا تمكنا بعون الله من نقل بطولات المجاهدين المنشورة في مواقع الحسبة والبراق والاخلاص واصدارت الجبهة و رسائل قائمة الانصار البريدية وروائع مؤسسة السحاب وغيرها من المواقع الجهادية كيف سيكون حال اعداء الاسلام قاتلهم الله.

ان المعركة كبيرة والمصاب فيها جلل وهي لحاجة لكل جهد مؤطر بالايمان بالله سبحانه وبهدي نبيه المصطفى صلى الله عليه وسلم ولاضرب لكم مثلا بسيطا على اهمية نشر افلام المجاهدين و سرعة انتشارها ففي احدى عمليات الجيش الإسلامي بالتعاون مع اخواننا في جيش المجاهدين فقد تم تصوير اسقاط الطائرة البلغارية و قتل من كان فيها و نشر فلم تنفيذ حكم الله في اخر طيار بلغاري في احد منتدياتهم عن طريق احد الاخوة هناك فشاهدها خلال زمن قصير اكثر من **30** الف زائر فكيف سيكون الحال ان يسرنا وصول مثل هذه العمليات الجهادية الى بيوت وعوائل جنود الكفر او من تحدثه نفسه التوجه الى بلاد المسلمين في أرض الرافدين وافغانستان لمقاتلة أسود الجهاد.

يقيننا بالنصر في جهادنا لملة الكفر ثابت لكن ذلك لن يتحقق ان لم نجهد انفسنا بالبحث عن كل صغيرة او كبيرة تعيننا في ان يأخذ اعلامنا الجهادي الدور المطلوب منه فعدونا ليس سهلا ابدا فبيده سلاح التقنية والتطور العلمي الهائل لكنه في قرارة نفسه يائس لا امل له بالنصر اما نحن فعندنا قبل العلم والتقنية ايماننا الكبير بعدالة القضية التي نقاتل دونها الا وهي رفع راية لا

اله الا الله قال تعالى " (وَعَدَ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَعَمِلُوا الصَّالِحَاتِ لَيَسْتَخْلِفَنَّهُم فِي الْأَرْضِ كَمَا اسْتَخْلَفَ الَّذِينَ مِن قَبْلِهِمْ وَلَيُمَكِّنَنَّ لَهُمْ دِينَهُمُ الَّذِي ارْتَضَى لَهُمْ وَلَيُبَدِّلَنَّهُم مِّن بَعْدِ خَوْفِهِمْ أَمْناً يَعْبُدُونَنِي لَا يُشْرِكُونَ بِي شَيْئاً وَمَن كَفَرَ بَعْدَ ذَلِكَ فَأُوْلَئِكَ هُمُ الْفَاسِقُونَ) (النور : 55)"

حفظ الله اهل الحسبة و البراق و الاخلاص و مجاهدي الجبهة و مشرفي قائمة الانصار البريدية و مؤسسة السحاب و كافة العاملين في الاعلام الجاهدي ممن سخروا وقتهم لخدمة هذا الدين .اللهم سدد رميهم و ثبتهم على الحق و احفظهم بعينك التي لا تنام .

الاثنين **6** – ذو القعدة **1427** هجرية

﴿ وَأَعِدُّوا لَهُم مَّا اسْتَطَعْتُم مِّن قُوَّةٍ وَمِن رِّبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ ﴾



العدد الأول - شهر ذو القعدة
سنة ١٤٢٧ هجرية

مجلة دورية تصدر عن مركز الفجر للإعلام

قريبا

من مركز الفجر :

1 - فلم أبناء المجاهدين من مؤسسة جند الله للمجاهدين الاوزبك

2 - فيلم جحيم المرتدين في الصومال



في مجلة المجاهد التقني تقرؤون :

1 - كيف تخفي شخصيتك على الانترنت.

2 - "برنامج أسرار المجاهدين" رؤية من الداخل.

3 - كيف تنشىء موقعاً جهادياً من الألف إلى الياء ؟

